

**IN THE DISTRICT COURT  
AT NORTH SHORE**

**CRI-2012-092-001647**

**UNDER THE EXTRADITION ACT 1999**

**IN THE MATTER OF A REQUEST BY THE GOVERNMENT OF THE  
UNITED STATES OF AMERICA  
FOR THE SURRENDER OF PERSONS IN NEW ZEALAND**

**UNITED STATES OF AMERICA  
Applicant**

v

**KIM DOTCOM  
MATHIAS ORTMANN  
BRAM VAN DER KOLK  
FINN BATATO  
Respondents**

Hearing: 21 September 2015 to 24 November 2015

Counsel: Ms C Gordon QC, Mr M Ruffin, Mr F Sinclair and Mr F Briggs  
for United States of America  
Mr R Mansfield, Mr S Cogan and Ms H Wild for Mr Dotcom  
Mr G Illingworth QC, Mr G Foley and Ms Hyde for  
Mr Ortmann and Mr van der Kolk  
Mr Batato for self  
Mr G Newell as Amicus Curiae

Judgment: 23 December 2015

---

**RESERVED JUDGMENT OF JUDGE N R DAWSON**

---

## **PART A**

### **Introduction**

[1] An application has been made by the United States of America (the applicant) for a determination that Kim Dotcom, Mathias Ortmann, Bram van der Kolk and Finn Batato (the respondents) are eligible to surrender to the United States to face criminal charges in that country for alleged criminal copyright infringement, money laundering, racketeering and wire fraud. The respondents defended the extradition application and filed three stay applications prior to the commencement of the eligibility hearing.

### **The Respondents**

[2] The respondents are officers of the Mega group of companies (Mega), which were registered in Hong Kong as incorporated companies. Their business operations principally involved cloud storage and file-hosting websites. Megaupload Ltd commenced business in 2005 as an internet service provider offering an online cloud storage service. A premium subscription allowed persons to upload, download and share files, which included movies and music content that were subject to copyright. Members of the public could access and download these copyrighted files once they were provided with the Uniform Resource Locator (URL) link. The charges arise out of the alleged reproduction and distribution of copyright infringing content by Mega's business operations.

### **The Provisional Arrest of the Respondents**

[3] On 13 January 2012 the Ministry of Foreign Affairs and Trade received diplomatic notes from the United States Embassy requesting the provisional arrest of the respondents for the purpose of extradition. In response to these provisional requests Crown Law, on behalf of the United States of America, filed with the North Shore District Court an application dated 17 January 2012 for provisional warrants for the arrest of the respondents, together with the appropriate supporting documentation. Judge McNaughton issued provisional arrest warrants against the respondents on 18 January 2012 who were subsequently arrested by the New Zealand Police on 20 January 2012.

[4] At the time of their arrests Mr Dotcom and Mr van der Kolk were New Zealand residents. All the respondents are currently on bail awaiting the outcome of these proceedings. Mega's business operations were shut down on 19 January 2012 when the United States Department of Justice seized control of the companies' websites.

### **Extradition Act 1999**

[5] The process for extradition from New Zealand is governed by the provisions of the Extradition Act 1999 (the Act), the terms of any relevant bilateral treaty New Zealand has entered into with another country and any applicable international conventions to which New Zealand is a party. Such bilateral treaties may stipulate the terms on which a person, who is the subject of a request for extradition (a requested person), may be extradited to and from New Zealand. The requested person is a person suspected of committing, or who has been convicted of, an extradition offence.

[6] For the purposes of this application New Zealand has an extradition treaty with the United States of America, which was promulgated as Extradition (United States of America) Order 1970 (SR 1970/240) (the Treaty). In terms of the Act, the United States of America is the requesting country in this case.

[7] Depending on the status of a requesting country different procedures under the Act apply to the extradition of a requested person from New Zealand. Part 3 of the Act specifies that the Act applies to extradition from New Zealand to certain treaty countries and certain Commonwealth and other countries. Due to the existence of an extradition treaty in this case the procedural provisions of Part 3 are applicable to the United States, as the requesting country.

[8] Under Part 3, once formal requests are received from the requesting country, the Minister of Justice may request a District Court Judge to issue a warrant to arrest the person whose surrender is sought. Thereafter, unless the Minister of Justice orders that the proceedings be discontinued under s 21(3) of the Act, the matter goes before the District Court which determines under s 24 whether the requested person

is eligible for surrender in relation to the offence or offences for which surrender is sought.

[9] On 28 February 2012 the United States, via a diplomatic representative, delivered four formal requests to the Ministry of Foreign Affairs and Trade for the surrender of the four respondents for extradition to the United States to stand trial on charges that include criminal copyright infringement, money laundering, racketeering and wire fraud.

[10] These formal requests were then transmitted to the Ministry of Justice. Upon receipt of these formal requests to surrender from the United States the then Minister of Justice, the Honourable Judith Collins, gave written notification of such matters, dated 1 March 2012, to the North Shore District Court under s 23(4) of the Act. Crown Law was ultimately instructed to prosecute the eligibility to surrender proceeding under the Act.

### **Eligibility Hearing**

[11] The hearing to determine whether a person is eligible for extradition takes place in the District Court pursuant to s 24 of the Act. Section 24 of the Act says:

#### **24 Determination of eligibility for surrender**

- (1) Subject to section 23(4), if a person is brought before a court under this Part, the court must determine whether the person is eligible for surrender in relation to the offence or offences for which surrender is sought.
- (2) Subject to subsections (3) and (4), the person is eligible for surrender in relation to an extradition offence for which surrender is sought if—
  - (a) the supporting documents (as described in section 18(4)) in relation to the offence have been produced to the court; and
  - (b) if—
    - (i) this Act applies in relation to the extradition country subject to any limitations, conditions, exceptions, or qualifications that require the production to the court of any other documents; or

- (ii) the terms of an extradition treaty in force between New Zealand and the extradition country require the production to the court of any other documents—

those documents have been produced to the court; and

- (c) the court is satisfied that the offence is an extradition offence in relation to the extradition country; and
  - (d) the court is satisfied that the evidence produced or given at the hearing would, according to the law of New Zealand, but subject to this Act,—
    - (i) in the case of a person accused of an extradition offence, justify the person's trial if the conduct constituting the offence had occurred within the jurisdiction of New Zealand; or
    - (ii) in the case of a person alleged to have been convicted of an extradition offence, prove that the person was so convicted.
- (3) The person is not eligible for surrender if the person satisfies the court—
- (a) that a mandatory restriction on the surrender of the person applies under section 7; or
  - (b) except in relation to a matter referred to in section 30(2)(ab), that the person's surrender would not be in accordance with the provisions of the treaty (if any) between New Zealand and the extradition country.
- (4) The court may determine that the person is not eligible for surrender if the person satisfies the court that a discretionary restriction on the surrender of the person applies under section 8.
- (5) Subsections (3) and (4) are subject to section 105.
- (6) Without limiting the circumstances in which the court may adjourn a hearing, if—
- (a) a document or documents containing a deficiency or deficiencies of relevance to the proceedings are produced; and
  - (b) the court considers the deficiency or deficiencies to be minor in nature,—

the court may adjourn the hearing for such period as it considers reasonable to allow the deficiency or deficiencies to be remedied.

[12] In addition the Court must be satisfied that the appropriate supporting documentation has been produced, that the offence is an extradition offence in

relation to the extradition country (the United States of America) and that there is sufficient evidence relating to the alleged offending that would justify the person's trial.

[13] Any applicable mandatory or discretionary restrictions on surrender will also be considered by the Court.

[14] Pursuant to s 25 of the Act, an exempted country such as the United States may present evidence through a record of case (ROC) procedure. Section 25 says:

**25 Record of case may be submitted by exempted country at hearing**

- (1) For the purposes of any determination under section 24(2)(d)(i), a record of the case may be submitted by or on behalf of an exempted country.
- (2) A record of the case must be prepared by an investigating authority or a prosecutor in an exempted country and must contain—
  - (a) a summary of the evidence acquired to support the request for the surrender of the person; and
  - (b) other relevant documents, including photographs and copies of documents.
- (3) The record of the case is admissible as evidence if it is accompanied by—
  - (a) an affidavit of an officer of the investigating authority, or of the prosecutor, as the case may be, stating that the record of the case was prepared by, or under the direction of, that officer or that prosecutor and that the evidence has been preserved for use in the person's trial; and
  - (b) a certificate by a person described in subsection (3A) stating that, in his or her opinion, the record of the case discloses the existence of evidence that is sufficient under the law of the exempted country to justify a prosecution in that country.
- (3A) A person referred to in subsection (3)(b) is—
  - (a) the Attorney-General or principal law officer of the exempted country, or his or her deputy or delegate; or
  - (b) any other person who has, under the law of the exempted country, control over the decision to prosecute.
- (4) Nothing in this section—

- (a) prevents an exempted country from satisfying the test in section 24(2)(d)(i) in accordance with the provisions of this Act that are applicable to countries that are not exempted; or
  - (b) limits the evidence that may be admitted at any hearing to determine whether a defendant is eligible for surrender.
- (5) A court to which a certificate under subsection (3)(b) is produced must take judicial notice of the signature on it of a person described in subsection (3A).

[15] If the Court ultimately determines that the person is eligible for surrender, the matter is referred to the Minister of Justice for a final decision. The person or requesting country may then exercise appellate rights to the High Court on any questions of law arising from the District Court decision.

### **Standard of Proof**

[16] Section 24(1) of the Act requires this Court to determine whether each of the respondents is eligible for surrender. Section 24(2)(d)(i) says this Court will be satisfied if the conduct constituting the offence would justify the respondents' trial on the charges if the offence had occurred within the jurisdiction of New Zealand. The applicant is required to produce sufficient evidence to satisfy each element of the Treaty offences, or if a New Zealand offence that is deemed a Treaty offence to the point where a finding of guilt could reasonably be reached at trial. This standard of proof is usually known as establishing a prima facie case.

[17] The duty of this Court is explained in *R v Governor of Pentonville Prison ex p. Osman*:<sup>1</sup>

... it was the magistrate's duty to consider the evidence as a whole, and to reject any evidence which he considered worthless. In that sense it was his duty to *weigh up* the evidence. But it was not his duty to *weigh* the evidence. He was neither entitled nor obliged to determine the amount of weight to be attached to any evidence, or to compare one witness with another. That would be for the jury at trial.

[18] Although this Court is not required to weigh the evidence, it does have the discretion to reject evidence that is manifestly unreliable.

---

<sup>1</sup> *R v Governor of Pentonville Prison ex p. Osman* [1989] 3 All ER 701 at 721.

[19] In *USA v Ferras*<sup>2</sup> the Supreme Court of Canada said:

[54] ... If the evidence is so defective or appears so unreliable that the judge concludes it would be dangerous or unsafe to convict, then the case should not go to a jury and is therefore not sufficient to meet the test for committal.

[20] In *United States v Tomlinson*<sup>3</sup>, the Court of Appeal for Ontario summarised the standard of proof as:

[47] ... that if there is some evidence, that is available for trial and not manifestly unreliable, on every essential element of the parallel Canadian crime, upon which a jury properly instructed, could convict, the test for committal will have been met. In that regard, it matters not whether the case against the person sought is “weak” or whether the prospect for conviction “unlikely”. The ultimate question of guilt or innocence is for the trial court in the foreign jurisdiction.

[21] In addition to providing evidence to a prima facie standard of proof, our Supreme Court in *Dotcom v USA*<sup>4</sup> has found that the requirements of natural justice under common law and under s 27 of the Bill of Rights Act apply to eligibility hearings. A person faced with extradition has to be fully informed of the case to be met and to have had a fair opportunity to respond to the case presented by the requesting state. These requirements are set out in the following paragraphs from Her Honour Elias CJ’s judgment in that case:

[50] The wider legislative context also includes the New Zealand Bill of Rights Act and the right to natural justice contained in s 27 of that Act. An interpretation of the record of the case to require provision of documents which are evidence of the necessary elements of an offence is consistent with the right to natural justice because such interpretation allows the person subject to the eligibility hearing to know the case against him and provides him with the opportunity to challenge any inferences not supported by the documents. The interpretation of s 25(2)(b) to require inclusion of such documents for reasons of natural justice is therefore to be preferred under s 6 of the New Zealand Bill of Rights Act.

...

[52] So it seems to me to be relevant when considering what natural justice requires in relation to a hearing to determine eligibility for surrender that s 24 for example requires that those charged are to be informed “in detail of the nature ... of the charge”, and are to have “the right to

<sup>2</sup> *USA v Ferras* [2006] SCC 33.

<sup>3</sup> *United States v Tomlinson* [2007] 219 CCC (3d) 97 (ONCA).

<sup>4</sup> *Dotcom v USA* [2014] 1 NZLR 355.



adequate time and facilities to prepare a defence”, together with rights to legal assistance and the assistance of an interpreter. They are rights that must apply to the necessary steps in the extradition process, such as the determination that a prima facie case is made out. Similarly, the minimum rights of criminal procedure, although expressed to be “in relation to the determination of the charge” include rights in relation to sentence and appeal and equally, in my view, are not to be confined to matters of trial alone, to the exclusion of critical steps along the way to determination of the charge. If so confined, the rights would be effectively eroded before the trial was reached. The right to a fair and public hearing by an independent and impartial court and to be presumed innocent until proven guilty for example are directly relevant to judicial determination of whether trial is justified. And the legislation is properly to be interpreted in conformity with these standards.

[53] Like the committal hearing on which the Extradition Act patterns it, the eligibility hearing is intended to provide opportunity to be heard on the question whether the threshold prima facie case has been demonstrated by the requesting state. Fairness requires that the subject of the proceedings has access to sufficient information to enable him to participate effectively at the hearing. That is the policy of the Criminal Disclosure Act also. In extradition cases, these policies may not support the disclosure appropriate to fair trial. But they suggest that fair hearing under Part 3 requires disclosure of the documents relied on to establish the elements of the offences charged for the purposes of the determination of whether there is a prima facie case. Where a record of the case is employed (so that documents included need no other proof), that context supports an interpretation of s 25(2)(b) that includes provision of copies of the documents relied on as evidencing the prima facie case.

[54] Against the background of the record of the case procedure, what is required is provision of material that is necessary to fairly inform the person the subject of the application of the evidence against him and provide him with the opportunity to test it to the prima facie standard envisaged. That is not simply a formal check on the assumption that the material in the record is accurate. (If so, the Part 3 procedure would be little different from the Part 4 procedure.) It is intended as an effective opportunity to answer the prima facie case.

...

[87] Because the requirements of natural justice in respect of the eligibility hearing are shaped by that hearing, disclosure relevant not to the determination of eligibility but to matters in issue at trial may not be appropriate for pre-hearing disclosure. I also accept, too, that in establishing a prima facie case the requesting country is entitled to identify the evidence it relies on. I see the scope of disclosure as generally limited to that evidence and material which bears on its reliability. ...

## **Counts in the Superseding Indictment**

[22] On 5 January 2012 a United States federal grand jury returned an indictment (the superseding indictment). The superseding indictment was filed with the United States District Court for the Eastern District of Virginia, and charged the four respondents, together with other individuals and corporate entities (including Mega), with conspiracy to breach copyright, conspiracy to racketeer, money laundering and wire fraud.

[23] A Judge of the US District Court on the same date authorised corresponding arrest warrants against each of the respondents named in the superseding indictment.

[24] The superseding indictment for each respondent contains thirteen (13) counts. The indictments are identical in all major respects and in summary allege the following offences:

*Count One:* Conspiracy to commit racketeering, in violation of Title 18, United States Code, Section 1962(d), which carries a maximum penalty of twenty years of imprisonment.

*Count Two:* Conspiracy to commit copyright infringement, in violation of Title 18, United States Code, Section 371, which carries a maximum penalty of five years of imprisonment.

*Count Three:* Conspiracy to launder monetary instruments, in violation of Title 18, United States Code, Section 1956(h), which carries a maximum penalty of twenty years of imprisonment.

*Count Four:* Criminal copyright infringement by distributing a copyright work being prepared for commercial distribution on a computer network, and aiding and abetting of criminal copyright infringement, in violation of Title 18, United States Code, Sections 2 and 2319(d)(2), and Title 17, United States Code, Section 506(a)(1)(C), which carries a maximum penalty of five years of imprisonment.

*Counts Five through Eight:* Criminal copyright infringement by electronic means, and aiding and abetting of criminal copyright infringement, each in violation of Title 18, United States Code, Sections 2 and 2319(b)(1), and Title 17, United States Code, Section 506(a)(1)(A), each of which carries a maximum penalty of five years of imprisonment.

*Counts Nine through Thirteen:* Fraud by wire, and aiding and abetting fraud by wire, in violation of Title 18, United States Code, Sections 2 and 1343, which carries a maximum penalty of twenty years imprisonment.

### **Mega History and Business Structure**

[25] Mr Dotcom and Mr Ortmann created Megupload Ltd in 2005. Mr Dotcom was the Chief Executive Officer of Megaupload Ltd until 2011 when he became its Chief Innovation Officer. He holds 68 percent of the shares in Megaupload Ltd; Mr Ortmann was the Chief Technical Officer holding 25 percent of the shares; Mr van der Kolk was employed by Mega as a computer programmer in 2005, he holds 2.5 percent of the Megaupload shares; and Mr Batato was employed by Mega in 2007 and was the Chief Marketing Officer but is not a shareholder in Megaupload. The three shareholder respondents in fact utilised holding companies to hold their shares in Megaupload.

[26] Mr Ortmann registered the domain name for Megaupload in 2005. Mr Dotcom registered Megaupload (Hong Kong) as a company later that year. The domain name for Megavideo was registered in 2000 by Mr Ortmann. Mr Dotcom registered the Megavideo company in 2006. Mr Dotcom owns all of Megavideo. Megavideo and Megaupload shared the same back-end database so both websites had access to the same underlying files.

[27] A number of other associated websites and businesses exist, including Megarotic (renamed Megaporn from 2008) and Megaclick.

[28] Mega grew rapidly and became very successful. It became one of the world's most successful internet service providers. At one stage it was estimated to:

- (1) Have more than 60 million registered users;
- (2) Have an average of 50 million daily visits;
- (3) Have over 65 million unique users from Brazil and over 30 million unique users from the United States;
- (4) Be the 13<sup>th</sup> most frequently visited site on the internet;
- (5) Account for approximately 4 percent of the total traffic across the internet;
- (6) Have had more than one billion unique visitors.

[29] Mega also became highly profitable. Its primary sources of income were from premium subscriptions from downloaders gaining access to stored files and online advertising. In the 2010 year it is estimated Mr Dotcom earned up to US\$42 million; Mr Ortmann up to US\$9 million; Mr van der Kolk up to US\$2 million; and Mr Batato up to US\$400,000.

[30] Carpathia Hosting Inc. formed the main backbone of the server network used by Mega. Carpathia provided server capacity in Virginia, USA, the venue for the criminal proceedings commenced in that state. Mega also leased or owned approximately 690 servers from Leaseweb, a multinational internet hosting provider with headquarters in the Netherlands.

[31] Server capacity was also obtained from Cogent in Washington, USA, and France. The Cogent servers provided a high-speed service to users. Mega utilised these servers to distribute files subject to high levels of demand.

[32] The Mega business allowed persons to upload files and to store them on the servers leased by Mega from Carpathia, Cogent and others who owned the physical

server networks. An URL would then be created which was a link through to the stored file. The uploader would use that URL to gain access to the stored file. They could also pass on the URL details to others to allow them to gain access to the file via the URL. The material so stored ranged from personal items such as family photos to commercial material such as music, videos, movies, video games and software. In late 2005, Mega commenced a rewards scheme to attract popular material. This acted as an incentive to users to upload files onto Mega servers and then publish the URL links on the internet providing access to the files. The URL link could be widely shared and downloaded by large numbers of people.

[33] Large numbers of files were uploaded to Mega by many different uploaders. Many of the files uploaded by different uploaders were the same files. Mega, like many others in the same industry, used a process of de-duplication in order to reduce the amount of storage space occupied by the same files. By the use of algorithms, Mega could identify when a file was being uploaded, whether that same file had been already uploaded and stored on the Mega site. In those cases, instead of storing the same file twice, or many times, it would be stored only once, but each uploader would have its own URL in order to gain access to the file. Popular files often had large numbers of URLs providing links to the same file.

[34] The service provided by Mega was dual use technology. That is to say, it could be used for entirely legitimate purposes (e.g. storing and accessing family photos) or for illegitimate purposes (e.g. storing and accessing copyright protected content in breach of the copyright owners' property rights). Most cloud storage and file hosting websites can be misused for illegitimate purposes. Mega, like others in the same industry, would receive takedown notices from copyright owners requiring them to remove the copyright protected files.

### **The Applicant's Case**

[35] The case against the respondents as officers of Mega recorded in the ROC and its supplements (SROC) is to the effect that:

- (i) Mega was directed by a small group, essentially those named in the superseding indictment. It is not plausible to suppose that major aspects of its operations were not known about and acquiesced in by these men.
- (ii) The volume of takedown notices, the need for the Abuse Tool, and Mega's public reputation all suggested that it hosted significant infringing content.
- (iii) The Megaupload database reveals many hundreds of thousands of copyright-infringing works on the Mega sites.
- (iv) In response to takedown action, Mega did not delete files or disable all access. It merely deleted the particular URL link identified by the copyright owner and did not notify the uploader of the takedown.
- (v) Most of the traffic to Megaupload and Megavideo was not direct (i.e. it did not involve visits in which the user has directly typed the URL link into the web browser or bookmarked to the URL link). The preponderance of traffic involved visits from referral sites, the most prolific of which were linking sites specialising in the provision of links to infringing material.
- (vi) Most of the traffic to Megavideo was associated with user accounts that had been the subject of at least one takedown notice (27.2 billion views or 77 percent of recorded views on the site).
- (vii) The sites were primarily used to view and download content. More than 90 percent of registered users had never uploaded a file to Megaupload or Megavideo.
- (viii) Viewing privileges were calibrated by reference to the length of commercial movies and were manipulated to encourage the purchase of subscriptions.

- (ix) Rewards were paid to flagrant repeat infringers who had uploaded obvious infringing content. That content was the subject of extreme numbers of takedown notices.
- (x) Despite the obvious indications that Mega's popularity was based on its infringing content, the Cogent system was developed. The most popular content was automatically identified and copied onto Cogent servers, which were better equipped to deal with high levels of simultaneous demand. Sampling of those servers indicates that more than 90 percent of content was infringing.

[36] It is alleged that these features alone are sufficient prima facie evidence that the respondents participated in an enterprise with the aim of providing mass access to copyright infringing files. That is made clear from the statements and actions of the respondents.

[37] The applicant alleges that the respondents set up an "innocent front end" with a "private back end" on their sites. Visitors to the public front pages ("innocent front end") would have found no indication of the vast array of popular and copyright infringing content held and accessed only by the private back end. No copyright infringing content was displayed on the innocent front end, creating an aura of innocence.

[38] Uploaders could store files, including copyright infringing content, in the private back end and post URL links to linking sites which provided access to the files. The applicant alleges that most of the traffic to Mega came in through this private back end and this was where Mega made most of its money.

### **The Respondents' Case**

[39] The respondents' case is that Mega was effectively a "dumb pipe" and not an "informed pipe". That is to say, Mega provided a storage service to its users that was copyright neutral and a substantial portion of the user files stored were non-infringing. Mega, like other storage providers, offered a takedown mechanism to remove offending content at the request of copyright owners.

[40] The respondents say that an internet service provider (ISP) cannot be liable for the activity of its users and that the courts have consistently focused on the infringer, not the technology. They accept that Mega operated an innocent front end and a private back end but say that there is nothing unlawful or covert in that.

[41] Their websites' policies, including the rewards programme and free viewing time limit (policies common to nearly all commercial internet service providers), they were not biased for or against copyright and nor were they required to be. They were only biased to encourage users to the site. If there were no users, then there would be no subscriptions or advertisers resulting in no income, and no commercial ISP.

[42] The respondents say that the applicant has selectively cherry-picked the evidence presented to this Court to paint a prejudicial and fundamentally biased picture of the activities of Mega.

[43] The respondents also say that if a file is found to be in breach of copyright, that does not mean that all URLs linking to that file are in breach of copyright.

[44] It is for this reason that it is the identified URL link that is deleted, not the underlying file. That means that other users who may be entitled pursuant to copyright to access the file can continue to do so on other URL links.

### **The Applicant's Evidence**

[45] A selection of the alleged conduct from the ROC and its supplements, and the inferences that the applicant says can be drawn from that evidence follows. Much of it is based upon retrieved Skype conversations between various respondents. The paragraphs referred to are the paragraphs from the ROC and SROC.

### ***Alleged Inculpatory Statements***

[46] The applicant submits that the following Skype conversations demonstrate the existence of an agreement to exploit copyright infringing content followed by the inference they say can be drawn.



*Perception of Legal Threats*

[47] Paragraph [148b):

On or about August 16, 2010, via Skype, DOTCOM told ORTMANN in German, "at some point a judge will be convinced about how evil we are and then we're in trouble. We have to make ourselves invulnerable." To prevent this possibility, DOTCOM suggested "a new hosting model" that would make Megaupload "independent from," its server hosting facilities, "Capathia or leaseweb." DOTCOM said that Megaupload "should set up a fleet of our own servers with multiple hosters (15 or more in several countries) and make us untouchable." DOTCOM was particularly concerned about the domain name, stating, "The domain is the only danger, but for that there is the megakey." ORTMANN responded, "to counter the justice system with technical methods is difficult at our size . . . a piratepay places a few GB backup on new servers and is back online, with 30+ PB that's a little more difficult." In this context, the acronym "PB" refers to petabytes of data. DOTCOM replied, "the file servers are not the issue here. The web and db servers are. This structure has to be secure." DOTCOM added, "none will impound 1000 file servers." ORTMANN responded, "as soon as the laws change, we will not survive with technical methods." ORTMANN also said, "if a US-court prohibits Cogent from providing us service, we will soon lose the vast majority of our connectivity worldwide." DOTCOM then reminded ORTMANN, "you should not log our chats ;-) too much shit in there." ORTMANN responded, "unfortunately Skype autologs them . . . I'm going to erase them all.

*Inference:* Mr Dotcom and Mr Ortmann appreciated that Mega operated unlawfully and was at risk of being shut down by a court.

[48] Paragraph [103jj):

On or about March 8, 2009, via Skype, DOTCOM asked ORTMANN, in German, "Have you got a minute? Let's talk about how we should prepare for lawsuits, should they ever happen." ORTMANN responded, "We need to take a look at how YouTube has dealt with that so far. Promise some kind of technical filtering crap and then never implement it." DOTCOM added, "We should already be hiring an attorney now, perhaps an in-house one, to get us prepared for anything."

*Inference:* Mr Dotcom and Mr Ortmann expected Mega would be sued over its copyright violations and they should respond by deceiving owners.

[49] Paragraph [103vv):

As described in Paragraph 38(n) of the Record of the Case, on or about July 8, 2010, DOTCOM sent an e-mail to ORTMANN and Echternach entitled "attention." In the e-mail, DOTCOM copied a link to a news article entitled "Pirate Bay and Megaupload Escape Domain Seizure by US," which discussed how, "[a]s part of an initiative to crack down on Internet piracy and

counterfeiting, the US Government recently took action against sites making available movies and TV shows.” DOTCOM wrote, “this is a serious threat to our business. Please look into this and see how we can protect ourselves.” He also asked, “Should we move our domain to another country (canada or even HK?).” ORTMANN responded, “We just have to continue to comply with the law, then nothing can happen – proper takedown processing is our lifeblood – doing country-specific takedowns would have jeopardized that.” Echternach then responded, “In case domains are being seized from the registrar, it would be safer to choose a non-US registrar[.]” And ORTMANN replied, “They were apparently seized at the ICANN level, which wouldn’t even protect foreign domains. But there is a good reason why they did NOT actually seize thepiratebay.com and megaupload.com: We have proper registration credentials. Sven [Echternach], can you compile a list of pre-seizure registration details of all the domains that were taken over? Let’s find out if all of them were misregistered or anonymized (remember that megaporn.com is currently anonymized”).

*Inference:* Mr Dotcom feared that Mega’s copyright violations would result in criminal sanctions.

[50] Paragraph [103f]:

On or about June 5, 2007, via Skype, VAN DER KOLK said to ORTMANN, “BTW, scary story about Kim wiring 50,000 dollars from the Megaupload account to his personal PH account...” The abbreviation “PH” appears to refer to the Philippines. ORTMANN responded, “I am wondering why Kim is taking this so lightly,” and “something fishy is going on.” ORTMANN commented, “if it was a U.S. authorities problem with Megaupload, we wouldn’t be doing business with PayPal any longer, that’s for sure.” VAN DER KOLK responded, “yeah indeed.” ORTMANN then stated, “Kim should refrain from travelling to the U.S., though.” And VAN DER KOLK replied, “yeah I wouldn’t go to the US either if I were him.”

[51] *Inference:* Mr van der Kolk and Mr Ortman appreciated that Mega’s copyright violations made it vulnerable to criminal sanctions and therefore it was unsafe for Mr Dotcom to travel to the United States.

[52] Paragraph [103i]:

On or about August 20, 2007, via Skype, VAN DER KOLK said to ORTMANN, “I mean if Kim was a solid guy with a good financial background and being safe with his money I wouldn’t mind, but the current situation is a bit risky in my opinion.” ORTMANN responded, “the good thing is, he is operationally dependent on us...he cannot sneak away with the money.” VAN DER KOLK then asked, “but what if shit really hits the fan ... would he grab the last little bit of money and take off ...he’s good at that.” And ORTMANN replied, “true ... but with his spending nowadays, he will attempt to get the shit off the fan, and that’s what he needs us for.” This Skype

conversation was contained in an e-mail sent by VAN DER KOLK to a third-party on or about August 21, 2007.

[53] *Inference:* Mr Van der Kolk and Mr Ortmann appreciated that Mega's operations were unlawful and they thought it likely that Mr Dotcom would abscond.

[54] Paragraph [134f]:

On or about May 6, 2009, via Skype, ORTMANN told VAN DER KOLK, "Ponzi scheme," and VAN DER KOLK responded, "yes that's Kim style indeed." ORTMANN replied, "worked well so far," "luckily," and VAN DER KOLK responded, "Most Ponzi schemes pay much more frequently though :)" Then VAN DER KOLK said, "yeah but the likeliness that we'll triple our profit again in 2010 is quite small," "while at the same time the likeliness of us getting in trouble for some reason is getting bigger." ORTMANN responded, "very true," and VAN DER KOLK replied, "and the fact is when there's no way out, Kim [DOTCOM] will also grab the last couple of millions and go on hiding mode again when that happens." ORTMANN responded, "yes," "or he'll spend them and then ask ME to save him." VAN DER KOLK replied, "HAHA" "how ironic," and ORTMANN responded, "I already see that coming."

*Inference:* Mr Ortmann and Mr van der Kolk appreciated Mega's copyright violations were unlawful and anticipated some form of legal trouble. They expected Mr Dotcom to abscond when that happened.

[55] Paragraph [103p]:

On or about October 7, 2007, via Skype, ORTMANN told VAN DER KOLK, "back in the early days, I hoped that we would stay online for 2, 3 more months," "before law enforcement would take our servers down..." VAN DER KOLK asked, "seriously? you were that sceptical?" And ORTMANN answered, "every day that passed without something serious happening on that side made me feel happy." VAN DER KOLK responded, "Amongst our sites Megaupload is definitely the safest legally I think." ORTMANN replied, "there is really no easy way to distinguish between an ISP and us." A few minutes later, VAN DER KOLK told ORTMANN that they should have a "backup payment provider," "but we're not super attractive to potential buyers or investors, and that's unfortunate." ORTMANN responded, "yes, although the new VC still seems to be interested." VAN DER KOLK asked, "that's good, but do you think it will really get to an investment?" ORTMANN responded, "if we were a 100% clean site with that growth and profit, we would have sold for a nine-figure sum already." VAN DER KOLK replied, "yes, unfortunately :- (" and then: "But what would make us attractive to VC's is if they could put in a bit of money so that we can grow and be sold to a big player in the future for much more money. We don't need money to grow (at least not with the current business model), and it will be hard to get sold to a big player because we're not 100% legit.." ORTMANN responded, "This is exactly the point where the higher-level suits always cancel the investment" "and they've got a point there..." VAN DER KOLK replied, "yeah that's very unfortunate, we have to think of a work around for that otherwise we'll never

cash in and we'll just end up with legal problems in a few years or other problems." He also stated, "this can not last forever I think." ORTMANN responded, "we have to create spinoffs, legit ones, and fuel those." The acronym "VC" refers to a venture capitalist.

*Inference:* Mr Ortmann knew Mega systematically violated copyright from the start of its operations and was vulnerable to legal action. He and Mr van der Kolk appreciated that legal difficulties were inevitable and Mega needed to develop "spinoffs" that were "legit" or they would "never cash in".

#### *Piracy Statements*

[56] Paragraph [103m]:

On or about September 2, 2007, via Skype, VAN DER KOLK said to ORTMANN, "we're modern pirates :-)". ORTMANN responded, "we're pretty evil, unfortunately", "but Google is also evil, and their claim is 'don't be evil.'" VAN DER KOLK replied, "yes!" Then VAN DER KOLK stated, "and the world is changing, this is the internet, people will always share files and download their stuff for free," "with or without Megaupload." ORTMANN responded, "yes... the content providers should just get a producer account and sign up for rewards."

[57] The applicant says Mr Ortmann and Mr van der Kolk accept the labels of "evil" and "modern pirates" are correctly applied to their business, but find comfort in the view that internet piracy is unavoidable and (to their minds) practised by others.

*Inference:* Mr Ortmann and Mr van der Kolk appreciated that Mega was a 'pirate' operation reliant on systematic infringement of copyright.

[58] Paragraph [103v]:

On or about January 4, 2008, via Skype, VAN DER KOLK and ORTMANN discussed an e-mail alerting the Mega Conspiracy to a potentially fraudulent website with a name similar to Megarotic.com. VAN DER KOLK commented, "haha people worieing about our name being pirated :)" ORTMANN responded, "we have a ton of parasitic domains." VAN DER KOLK replied, "yeah I know, but the term piracy is funny in this context :)" because "we are the pirates here." ORTMANN responded "you can see it this way :)" but "no, we're just a service provider." VAN DER KOLK replied, "yeah legally, but we know better :)"

*Inference:* Mega was a vehicle for copyright piracy, which was concealed by a façade of legality.

[59] Paragraph [103w]:

On or about March 14, 2008, via Skype, ORTMANN told VAN DER KOLK, “we are in a strange business.” VAN DER KOLK responded, “yes indeed,” “modern day pirates :)”

[60] Paragraph [103ii]

On or about March 7, 2009, via Skype, VAN DER KOLK sent ORTMANN an e-mail from the Dutch organization BREIN (Bescherming Rechten Entertainment Industrie Nederland), “the Dutch anti-piracy program,” notifying Mega of a particular copyright infringing file on Megaupload.com. The e-mail was sent by a particular BREIN representative (hereinafter “PH”). VAN DER KOLK then said, “I had a lot of trouble with this [PH] guy :)” “with this mp3 site I had.” He continued, “They wanted to sue me, and only if I would sign a contract they would not,” but “then I left to Manila :)” and “never heard anything from them.” ORTMANN commented, “until now!” VAN DER KOLK added, “I had the top40 with direct downloads,” and ORTMANN responded, “that’s not so legal, of course :)” VAN DER KOLK then said, “always lived from piracy :)”

*Inference:* Mega’s business was copyright piracy.

[61] Paragraph [103mm]:

On or about March 16, 2009, via Skype, ORTMANN and VAN DER KOLK discussed the possibility of establishing a new Mega website for music without any copyright-infringing materials. ORTMANN said, “can’t wait to approach the music industry with requests to sell their products legally... ‘what?! yooooou???’” VAN DER KOLK responded, “haha” “If they at all want to do business with us.” He added, “If I were in that industry I would ban any Mega\* company :)” ORTMANN commented, “yep :)”

*Inference:* Mega’s business was copyright piracy.

[62] Paragraph [148f]:

On or about October 6, 2010, via Skype, ORTMANN sent DOTCOM a link to the agenda for the 2010 International Law Enforcement IP Crime Conference, which was co-hosted by Interpol and Hong Kong Customs and located at the Hong Kong Grand Hyatt Hotel, the Mega Sites' headquarters. ORTMANN commented in German, "in the lion's den."

*Inference:* Mega’s business was copyright piracy.

[63] Paragraph [134d]:

On or about April 2, 2009, via Skype, VAN DER KOLK told ORTMANN, “France accepted the controversial anti piracy law where they will disconnect users. But that’s only good for us as it will mainly affect p2p piracy.” ORTMANN responded, “unless they assume that all traffic from us is piracy or sniff peoples’ download URLs, it’s kinda hard to catch someone using MU/MV for piracy form a purely technical perspective.” To which VAN DER KOLK replied, “yes.”

*Inference:* The infringing content hosted by Mega was known to attract significant traffic.

*Embedded Players and Copyright Infringement*

[64] The applicant alleges that the embedded player function is explained in the ROC this way.<sup>5</sup>

According to e-mail and Skype conversations, members of the Mega Conspiracy permitted users of the Mega Sites to “embed” videos on third-party websites. Embedded videos were hosted on, that is, reproduced and distributed by, the Mega Sites but could be viewed and accessed from third-party linking sites. In other words, users could view Mega-hosted videos on third-party linking sites, but the Mega Conspiracy maintained direct control over the distribution of the underlying video file.

[65] The applicant alleges that the traffic flowing to Mega through embedded players was measured. In May 2007 Mr van der Kolk told Mr Ortmann that there were more than a million daily views via embedded players.<sup>6</sup> Less than a year later, he reported (paragraph [107g]):

... “almost 18.000.000 video views on MRV per day,” “and also a whopping 6.000.000 on MV now.” ORTMANN responded, “amazing” and “wow.” VAN DER KOLK added, “MV had nice growth during the past 2 months,” “probably piracy in embedded players” — “50.000 daily clicks topartypoker from the ads in the embedded players of MV.” ORTMANN responded, “that’s a massive asset,” and VAN DER KOLK replied, “yes,” “piracy or not :)” The website PartyPoker.com provided online gambling services.

*Inference:* It was known that Mega derived substantial growth from traffic to pirated content.

---

<sup>5</sup> SROC 2 para [107a] (ROC bundle p 157).

<sup>6</sup> SROC 2 para [107] (ROC bundle p 157).

[66] The applicant alleges that earlier in 2007, messages passing between Mr Ortmann and Mr van der Kolk expressed a degree of disquiet with the extent of “piracy” occurring through embedded players. Mr van der Kolk indicated that virtually all the content being accessed was infringing. Deleting files that were not “legit” would result in the loss of “99.999” of content.<sup>7</sup> The problem was “almost no harmless stuff is being uploaded to MV”.<sup>8</sup> In the end, no steps were taken to delete such material, and reliance was placed on the inability to search and identify infringing files directly on the Mega sites. At this early stage, then, it was decided that infringing material could safely be preserved on Mega servers.

*Inference:* Mega’s traffic was substantially based on users accessing copyright infringing files.

[67] Paragraph [107c]:

On or about May 23, 2007, via Skype, VAN DER KOLK asked ORTMANN, “If we identify a video as copyright, should we remove it only from the site or also make it unavailable in the embeded player?” ORTMANN responded, “that’s a very good question.” VAN DER KOLK replied, “I think it make sense to keep it available in the embeded players (at least for now).” ORTMANN responded, “I guess so, too,” and VAN DER KOLK replied, “okay.” Although VAN DER KOLK referred to “remov[ing]” copyright-infringing videos from the Mega Sites, these videos were not actually removed. Instead, these videos were simply marked “private.”

[68] Paragraph [107d]:

On or about August 30, 2007, via Skype, ORTMANN asked VAN DER KOLK, “how clean are the existing videos on MRV now, what do you think?” The acronym “MRV” appears to refer to the streaming section of Megarotic.com. VAN DER KOLK responded, “it’s pretty clean from the perspective of child porn / disgusting stuff,” “but still lot’s of copyright infringements.” He added, “if we want to clean things up we have to agree on what has to go and what not,” “otherwise I can delete 90% of the content :-)” Then VAN DER KOLK said, “right okay,” “so videos longer than 10 minutes on MRV should be set to private or something...” and ORTMANN responded, “yes,” but “direct linking / embedding is fine.” VAN DER KOLK added, “embedded players are not so harmful.” ORTMANN commented, “searchability is dangerous and will kill us,” and VAN DER KOLK replied, “yeah.”

---

<sup>7</sup> SROC 2 para [107f] (ROC bundle p 159).

<sup>8</sup> SROC 2 para [107xx] (ROC bundle p 143).

*Inference:* There was so much infringing content on the sites that its presence had to be disguised and made non-searchable. Traffic flowed to this content through third party sites.

[69] Paragraph [107e]:

On or about October 4, 2007, via Skype, VAN DER KOLK suggested to ORTMANN, “We should be a bit more careful with deleting popular videos from MRV in my opinion,” “since that is profitable.” ORTMANN responded, “so far, all case I have seen were MV,” “but you’re right, a popular MRV video should be mirrored to other servers rather than deleted :)” VAN DER KOLK replied, “yeah those are the long full dvd rips in embedded players, we really needed this feature,” and ORTMANN agreed, “yes, it was overdue.”

*Inference:* Mega ensured that infringing content remained available for distribution and was not deleted.

[70] Paragraph [107f]:

On or about October 7, 2007, via Skype, VAN DER KOLK said to ORTMANN, “Maybe we should automatically delete videos on Megavideo that are longer than 30 minutes and have more than XXX views or something because I still see so much piracy that is being embedded.” VAN DER KOLK then asked, “What kind of videos are legit and longer than 30 minutes and views more than XXX times...” ORTMANN responded, “what we can indeed do is put them into ‘temporarily not available’ state and priority-audit them” and “anything that’s legit will then be unblocked permanently, the rest will go to deleted.” VAN DER KOLK responded, “yeah, but 99.999% will be deleted then.” Based on a preliminary review of the Mega databases and source code, as of January 19, 2012, it does not appear that the Mega Conspiracy implemented a copyright screening feature for videos longer than 30 minutes based on the number of views.

*Inference:* Megavideo’s longer content was overwhelmingly copyright infringing.

[71] Paragraph [103rr]:

On or about October 10, 2009, via Skype, VAN DER KOLK told ORTMANN, “Theoratically we could make MV just like MU,” “remove all the video listing stuff.” ORTMANN responded, “yep, but even better than that, we list only really harmless stuff,” and VAN DER KOLK replied, “yes, but problem is almost no harmless stuff is being uploaded to MV :)” Then VAN DER KOLK suggested, “We should actively add youtube videos again perhaps,” and ORTMANN responded, “yes, we could do that indeed.” ORTMANN suggested, “Kim’s idea of leaving the semi-harmful stuff online for 23 hours is also pretty good,” and VAN DER KOLK responded, “yes also not bad,” “but then there will always still be harmful content on the site



always,” and “I would say we should not even make it public at all,” because “we make money from direct links & embedded, no need to risk anything.” ORTMANN responded, “harmful content isn’t bad per se as long as we process takedowns and don’t upload it ourselves.” VAN DER KOLK replied, “that we already do now even :)” and ORTMANN responded, “it has a positive effect in that it allows content owners to search our site and send takedown requests.” Then VAN DER KOLK said, “but it’s good to stay off the radar by making the front end look like crap while all the piracy is going through direct links & embedded.” And ORTMANN added, “the important thing is that nobody must know that we have auditors letting this stuff through.” VAN DER KOLK responded, “yes that’s very true also.” ORTMANN replied, “if we had no auditors – full DMCA protection, but with tolerant auditors, that would go away.” And VAN DER KOLK replied, “yes true.”

*Inference:* Megavideo’s content was almost entirely infringing and traffic flowed through it to third party sites. A lenient auditing process meant that this content was knowingly hosted. This state of affairs was deliberately concealed.

[72] Paragraph [103g]:

The Mega Conspiracy redirected all known URL links pointing to pornographic files from Megaupload.com to Megarotic.com. On or about July 1, 2007, via Skype, ORTMANN said to VAN DER KOLK, “I am thinking about the MU->MR file move... we should definitely put up an informative page when a user clicks on a MR link via the MU domain.” The acronym “MU” refers to Megaupload.com, and the acronym “MR” refers to Megarotic.com. ORTMANN then said, “yes... we could, however, also be shooting ourselves in the foot with this, as it proves that we looked at the file,” “and therefore are not the dumb pipe we claim to be.” ORTMANN also said, “copyright owners may use this against us.” VAN DER KOLK responded, “dangerous move indeed.”

*Inference:* Infringing content was knowingly hosted. Care had to be taken so that copyright owners were given no hint of this fact.

#### *Reliance on Copyright Infringement*

[73] Paragraph[103j]:

On or about August 30, 2007, via Skype, ORTMANN said to VAN DER KOLK, “as we’re displaying viewcounts, the copyright industry could be tempted to send us invoices for lost revenue based on that.” VAN DER KOLK responded, “that will hurt.” And ORTMANN replied, “indeed.”

[74] Paragraph [103k]:

On or about August 30, 2007, via Skype, VAN DER KOLK sent ORTMANN a URL link to Megavideo.com's most viewed videos for that day. VAN DER KOLK stated, "most viewed videos are all > 1 hour." ORTMANN responded, "that's a bad direction we're going in." And VAN DER KOLK replied, "yes.."

The applicant says that Mr van der Kolk and Mr Ortmann know that most Megavideo traffic was to infringing copies of commercial movies.

*Inferences:* Infringing content was knowingly hosted and Megaupload knew the infringing content had monetary value that was lost to the legitimate owners because of the group's conduct. Much of Megavideo's traffic was clearly due to infringing files of commercial video content.

[75] Paragraph [103hh]:

On or about March 7, 2009, via Skype, VAN DER KOLK said to ORTMANN, "If copyright holders would really know how big our business is they would surely try to do something against it," "they have no idea that we're making millions in profit every month." ORTMANN responded, "indeed."

*Inference:* Mega was highly profitable. This was known to be the result of hosting copyright infringing files whose actual owners were not being compensated for their intellectual property.

[76] Paragraph [103q]:

On or about November 14, 2007, via Skype, DOTCOM said to ORTMANN, in German, "will you eventually solve the conversion problem? the complaints don't stop. what do you think you can do?" ORTMANN responded, "we have a long queue of dvd-rips" "and some DRM protected, that cannot be converted." DOTCOM replied, "then we need more conversion servers", "please order." The acronym "DRM" refers to "Digital Rights Management" and is commonly understood to mean copyright-protection based in either software, such as encryption, or somewhat less commonly, hardware. During that time period, the Mega Conspiracy was converting user-uploaded videos, including copyrighted videos, into a particular video format known as Flash Video or "FLV," which facilitated the video's distribution.

*Inference:* Deliberate steps were taken by the group to achieve the mass distribution of copyright infringing content.

[77] Paragraph [103dd]:

On or about March 2, 2009, via Skype, NOMM told ORTMANN, “seems there are certain conditions to have ot HD encoded,” and ORTMANN responded, “BD rips :)” The term “HD” refers to high definition, and the term “BD rips” refers to infringing copies of Blu -ray Discs. NOMM then said, “I doubt youtube has any open rips hehe,” “we have ONLY movies/etc, they have very less such things :)”

*Inference:* Mega hosted content that was known to infringe copyright.

[78] Paragraph [103ee]:

[79] On or about March 2, 2009, via Skype, NOMM told ORTMANN, “seems there are certain conditions to have ot HD encoded,” and ORTMANN responded, “BD rips :)” The term “HD” refers to high definition, and the term “BD rips” refers to infringing copies of Blu -ray Discs. NOMM then said, “I doubt youtube has any open rips hehe,” “we have ONLY movies/etc, they have very less such things :)” On or about March 3, 2009, via Skype, VAN DER KOLK sent ORTMANN the results of a search for the term “1080p” in the Mega database. The term “1080p” refers to high-definition video, which typically contains 1080 lines of progressively vertical resolution. The search showed that the term appeared in more than 41,000 separate files. VAN DER KOLK sent ORTMANN some of the results, which included the copyrighted motion pictures “Transporter 2,” “The ForbiddenKingdom,” and “Ghost in the Shell: Stand Alone Complex — The Laughing Man.” ORTMANN commented, “yes :) but with HD video, we’ll easily need 50 gigs more already,” “but we’ll also be MUCH more popular/valuable.” VAN DER KOLK asked, “Kim likes the idea as well I suppose?” and ORTMANN responded, “he loves it.” Then ORTMANN asked, “I just wonder what warner bros. will say when they see crystal clear BD rips instead of the usual blurry video :)” and VAN DER KOLK responded, “yeah will be even more pissed off :)”

*Inference:* Mega hosted content that was known to infringe copyright.

[80] Paragraph [103oo]:

On or about March 20, 2009, via Skype, DOTCOM and ORTMANN discussed providing high definition content on Megavideo.com. DOTCOM said, in German, “I’m looking forward to MV [HD,]” “it will be cool.” ORTMANN responded, “The quality is going to be amazing ... the Warner Brothers opening credits for Terminator 3 on Andrus’ [NOMM] unoptimized demo video is already a feast for the eyes.” “Terminator 3: Rise of the Machines” is a copyrighted motion picture.

*Inference:* Copyright infringing content was knowingly hosted and redistributed in a format attractive to users.

[81] Paragraph [102qq]:

On or about May 25, 2009, via Skype, ORTMANN told NOMM, “H.264 will kill the movie industry the way that MP3 has killed the music industry,” “pure eye candy.” A few minutes later, VAN DER KOLK asked ORTMANN, “What will be the HD launch page?” and ORTMANN replied, “a landing page advertising ‘Megavideo goes High Definition,’” VAN DER KOLK responded, “Hollywood will curse us :)” and ORTMANN replied, “this is indeed the point where streaming web video is starting to rival theatre quality.” The term “H.264” refers to a particular standard for video compression that is commonly used in the compression and distribution of high definition videos.

*Inference:* The distribution of high definition copyright video took place on a scale that was damaging to the movie industry.

[82] Paragraph [103gg]:

On or about March 5, 2009, via Skype, ORTMANN told VAN DER KOLK, “MV has the potential to rock 2009 (and 2010).” VAN DER KOLK responded, “yes,” “what started as a youtube clone...” ORTMANN then said, “yep :) the MU business model works very well for online video (private links)” “now we’re doing exactly what I foresaw in the beginning – innocent front end, private back end :)”

*Inference:* Mega disguised its distribution of copyright content by maintaining an appearance of legitimacy, while piracy was known to be fostered by the publication of links on third party sites.

[83] Paragraph [103kk]:

On or about March 8, 2009, via Skype, ORTMANN and VAN DER KOLK discussed an e-mail from a user seeking technical support about the Mega sites. ORTMANN said, “uhm, the guy does have an IMDB entry :)” and then, “haven’t seen any of his works, but yes, he seems to be very active,” “we do have legit users.” VAN DER KOLK responded, “yes, but that’s not *what we make \$ with* :)” The acronym “IMDB” refers to the Internet Movie Database, available at IMDB.com, an online database of information relating to motion pictures, television programs, and video games.

*Inference:* Mega’s revenue relied on traffic to pirated content.

[84] Paragraph [103tt]:

On or about November 21, 2009, via Skype, ORTMANN told VAN DER KOLK, "MV's public videos could not possibly have generated significant payments."

*Inference:* Mega's revenue relied on traffic to pirated content.

[85] Paragraph [103ll]:

On or about March 9, 2009, via Skype, NOMM told ORTMANN, "one my friend said me:" "megavideo is major serials/etc supplier ... but why dont they supply subtitles to download?" NOMM added, "seems people think we are some movies download center lol." The acronym "lol" generally means "laugh out loud."

*Inference:* Mega hosted content that was known to infringe copyright.

[86] Paragraph [103uu]:

On or about November 30, 2009, via Skype, ORTMANN sent VAN DER KOLK the following e-mail submitted by a Mega user: I visit the website <http://www.watch-movies-online.tv> to watch some movies. The movies I can watch through so many mediums made available. However from my assessment, Megavideo gives better picture quality with minimal bufferings. ... VAN DER KOLK responded, "nice :)" "not many competitors with such massive bandwidth and such a conversion infrastructure." ORTMANN replied, "yes, and such a persistent group of nerdy Turks perfectionizing the conversion process :)" VAN DER KOLK also said, "okay, so we should definitely not piss off our uploaders now :)" and ORTMANN responded, "let's pay them to keep them happy." VAN DER KOLK replied, "yes indeed."

*Inference:* Mega facilitated access to infringing content on a mass scale.

[87] Paragraph [38I]:

On or about May 25, 2009, NOMM sent an e-mail to DOTCOM and Ortmann entitled "status report." Nomm wrote, "I have been processing HD videos for some time now to find best of the best for showcase (Mathias gave specification). Even though we have lots of HD content uploaded most seems to be problematic quality or legality wise." The term "HD" refers to high definition content.

*Inference:* Mega's High Definition content was known to infringe copyright.

[88] The applicant submits Andrus Nomm confirms that his co-conspirators were "aware that they were making money directly from reproducing and distributing copyright-infringing content uploaded to Mega Sites". This included millions of

dollars made through advertisements posted on the Mega Sites through Megaclick.com.<sup>9</sup>

*Payment of Rewards to Flagrant Repeat Infringers*

[89] The applicant alleges that:

- (i) From September 2005 until July 2011, Megaupload offered a rewards programme to premium subscribers whose URL links were used in high numbers of downloads by other users. These rewards were either money or subscription privileges.
- (ii) The scale of payment varied over time but, to earn cash rewards, uploaders had to attract a very large number of downloads associated with their links. The conditions of the scheme are produced in ROC paragraph 25.
- (iii) The rewards scheme is a self-contained case study of the conspiracy to defraud which makes out the offence under Art II.16 of the Treaty. Messrs Dotcom, Ortmann and van der Kolk directed the implementation of the rewards scheme. Mr Batato was a party to this offending. The rewards scheme, however, should not be viewed in isolation. The respondents' conduct must be measured against their knowledge of:
  - (1) The high volume of copyright material on Mega servers;
  - (2) The volume of internet traffic to that content, especially via linking sites;
  - (3) The high level of concern from copyright owners; and
  - (4) The function of linking sites in disseminating links to copyright material.

---

<sup>9</sup> SROC 6 para [170n] (ROC bundle p 310).

### **Summary of Applicant's Points**

[90] Mr Ortmann and Mr van der Kolk administered the scheme, with oversight and occasional intervention by Mr Dotcom. To meet the high download thresholds for obtaining payments, uploaders stocked their portfolios with popular, copyright infringing material. The traffic targets served as an incentive for uploaders to publish their links widely on the internet, in particular on the 'linking sites' that served as the de facto indices of Mega's content.

[91] Infringing content hosted by Mega was sometimes detected by copyright owners, who served notices against that content. Some conspicuous repeat infringers were the subject of thousands of takedown requests – in some cases hundreds of thousands. The scale of infringement by these conspicuous offenders was easily ascertained from Mega's database records, which enabled offending links to be associated with individual users. These individuals were flagrant "repeat infringers", whose accounts should have been terminated if Digital Millennium Copyright Act 1998 (DMCA) protection were to be claimed. The respondents continued to attract, reward and protect these individuals. This conduct demonstrates the conspiracy to defraud by causing deliberate injury to the proprietary rights of copyright owners.

[92] The respondents did this because there was a shared understanding that, especially in its early "growth phase" of the business, the illicit content of paid uploaders was vital to revenue. The portfolios of rewards claimants were examined before payment and Mr Dotcom sometimes directly commented about individual claimants. Mr van der Kolk often reported the contents of claimants to Mr Ortmann. These communications show that money was knowingly paid by Mega to individuals for infringing content. It was clearly appreciated that traffic volumes were related to the popularity of such content.

[93] The biographies of repeat infringers show Mega (in particular Mr van der Kolk) repeatedly paying individuals while also ineffectually processing takedown notices against their content. At least some repeat infringers were well known to Messrs Dotcom, Ortmann and van der Kolk. They corresponded with them, and analysed their activities and the traffic they brought to the business.

[94] Some of the respondents' dialogue concerned the cost of paying rewards. In the early days of the scheme, they tried to reduce this expense by selectively disqualifying reward claimants. This was occasionally excused on the grounds that portfolios contained infringing content. Although payments might be denied on this basis, the infringing content was not removed. This was in spite of the fact that the repeat infringer responsible for the uploads was known. Nor were users' accounts clearly terminated for reasons of copyright infringement. This was purely an economy measure. The respondents were interested in reducing an expense, not losing the traffic to popular content.

[95] Consideration was also given to targeting reward payments on the basis of subscription revenue generated by a user's content. This demonstrates how closely the main uploaders were studied, though no steps were taken to terminate the repeat infringer or delete their content. Disqualifying for content reasons was perceived as a risk to growth and an inefficient use of time. From at least 2008, so-called "sliders" were applied to falsify the download or view counts, and so reduce the apparent entitlement to payments. Disqualification for "fraud" is sometimes mentioned. This does not refer to the fraud of copyright infringement but, rather, frauds on the rewards scheme – for instance, by the use of software that caused continuous downloads of files and so falsified a claimant's traffic score.

[96] In total, at least US\$3 million was paid as cash rewards. Expenditure on rewards was kept to modest levels by the practice of disqualifying claimants or imposing the "slider" to manipulate rewards points. Disqualification implies examination of the claimants' portfolios. The content associated with an uploader was originally visible on Megaupload. In about November 2010, this feature was removed and the source of the content made anonymous. This step was taken to protect infringers (and Mega) from action by copyright owners.

[97] When the rewards scheme ended in 2011, Mr Dotcom wrote to PayPal and complained about the "criminal activity" of competitors who paid rewards – in the same manner as Mega had done for the past six years.



[98] The modus operandi of prolific uploaders illustrates certain aspects of Mega that are developed in the evidence. For example:

- (1) The creation of multiple links to a particular file.
- (2) Links were monitored and replenished if they had been deactivated in response to takedown activity.
- (3) It was known the “Megamanager” software, which Mega made available, assisted the activities of repeat infringers.

[99] Although the rewards scheme has been justified as a measure to encourage creative users to upload attractive user-generated content, this was clearly not its primary function. When the scheme was announced it was addressed to “file traders”. One condition of the rewards scheme was a 100 MB file size limit. A cursory glance reveals the spurious nature of this condition as full length motion pictures were constantly uploaded. Indeed, they at one point reprimanded uploaders for “splitting” larger files into smaller portions so as to receive more reward points when other users were forced to download each part of the whole.

*Scale of Infringement Through Content of Repeat Infringers*

[100] Mega’s databases would have enabled the ready identification of users who were repeat infringers. Paragraph [45b] explains:

On or about January 19, 2012, the FBI executed search warrants in Virginia and Washington, D.C., at locations where the Mega Conspiracy leased computer servers for the Mega Sites. Computer specialists with the FBI copied data from these servers, including multiple databases containing information about the Mega Sites. As stated in Paragraphs 31 and 32 of the Record of the Case, these databases contain information about the files uploaded to the Mega Sites, including, among other things, the following: file name; file extension type (*e.g.*, .avi, .jpg, etc.); file size; date; the file’s MD5 hash; whether a link to the file had been removed for abuse (including for copyright infringement); and the file’s 8-digit download identifier for use with the URL link (for example, the last eight digits of the following: [www.megaupload.com/?d=BY15XE3V](http://www.megaupload.com/?d=BY15XE3V)). In addition, the databases contain information about who uploaded a particular file, including, with respect to registered users, the user’s name, address, e-mail address, and username.

[101] Paragraph [46c] continues:

A preliminary analysis shows that the databases contain records of virtually every file available on Megavideo.com and Megaupload.com on or about January 19, 2012, the URL links associated with those files, and information about which users uploaded the files and associated links. Where multiple URL links pointed to the same file, the databases identify which user created each link and whether that link has been the subject of a copyright takedown request. For any given registered user, the databases identify every file and link uploaded by that user, including files and links that have been the subject of a copyright takedown request. The databases therefore provided the Mega Conspiracy with sufficient information to identify repeat infringers.

[102] Paragraph [46k] provides a breakdown of traffic to Megavideo involving user accounts that had URL links disabled through copyright infringement notices. There were 93,878 user accounts that had at least 1 URL link disabled as a result of takedown notices. Links created and distributed by these accounts, which included copyright-infringing materials, attracted more than 27.2 billion views (roughly 77 percent of the total views ever recorded on Megavideo.com).

[103] Other categories are represented in the table below.

No of user accounts	Links disabled	Views	Percentage of Megavideo total views
33	>10,000	475m	1.36 %
641	>1,000	5b	14.32 %
4,437	>100	12.8b	36.67 %
19,091	>10	19.8b	56.16 %

Taking ten takedown notices as a point of reference for “repeat” infringement, more than half of the recorded traffic to Megavideo can be associated with the infringing content of repeat infringers.

*Inferences:* Most traffic can be associated with the content of repeat infringers. Mega kept records that would easily have identified repeat infringers.

[104] Paragraph [106c]:

As stated in Paragraph 25(f) of the Record of the Case, on or about February 22, 2007, VAN DER KOLK sent an e-mail to ORTMANN entitled “2 reward payment files.” Attached to the e-mail was a text file listing proposed reward amounts, which ranged from USD \$100 to USD \$500, the Megaupload.com

username, and a description of the uploaded content. For a particular repeat infringer and unindicted conspirator (herein referred to as “AR”), VAN DER KOLK wrote the following: “Our old famous number one on MU, still some illegal files but I think he deserves a payment.” On or about April 6, 2007, via Skype, VAN DER KOLK said to ORTMANN, “[AR] uploaded a video! :-)”. ORTMANN responded, “YEAH :)” and then stated, “that is the breakthrough.” VAN DER KOLK replied, “our [old] famous reward participant.” ORTMANN commented, “he will upload tons from now on.”

*Inference:* Payments were made to encourage the uploading of infringing files.

[105] Paragraph [103e]:

On or about May 21, 2007, via Skype, ORTMANN said to NOMM, “but I have a feeling that Kim [DOTCOM] tolerates a certain amount of copyright violation.” NOMM responded, “yep but not too obvious ones.” ORTMANN then said, “since it helps initial growth,” “but we must not overdo it.”

*Inference:* Growth of the business was understood to be related to the hosting of infringing files.

[106] Paragraph [106d]:

On or about April 10, 2007, via Skype, VAN DER KOLK said to ORTMANN, “we should definitely pay all of the uploaders in the beginning,” and, “they will make us big.” ORTMANN then asked, “are new uploads currently audited for copyright violation?” VAN DER KOLK responded, “not yet, I am sending specs to Andrus [NOMM] shortly.”

*Inference:* Payment of rewards was expected to drive growth, without regard to the copyright status of the uploaded content.

[107] Paragraphs [106e] and [106f]:

The Mega Conspiracy’s Uploader Rewards program paid users for every download of their files. Many repeat infringers responded by splitting copyright-infringing videos into multiple parts and forcing users who wanted to watch the entire video to download each part. This increased their reward points.

On or about November 18, 2007, via Skype, VAN DER KOLK said to ORTMANN that a particular repeat infringer and unindicted conspirator (herein referred to as “VF”), “created a second account [NAME REDACTED] and within 19 days a 1500 USD redemption.” ORTMANN responded, “amazing” “we are very, very lucky to have him as an uploader.” ORTMANN then said, “those 1500 USD are multiplied by a factor of 10 at least” “and no DMCA notices yet from Vietnam.” VAN DER KOLK responded, “those are

well worth it, however major split files in the portfolio.” VAN DER KOLK then searched VF’s account based on file size and ORTMANN commented, “damn!!” “10000 46 MB files!” VAN DER KOLK responded, “yeah totally amazing.” And ORTMANN replied, “this guy is amazingly valuable.” VAN DER KOLK suggested, “It would be interesting if we can create statistics how many unique premium users downloaded a user’s files or how many ‘premium reward points’ a user has for the decision if a user should get paid or not...” He then said, “but yeah that would be too much work for now :)” ORTMANN responded, “I did make such statistics a year ago for some of our top uploaders” and “it turned out that one of the vietnamese guys generated several 10k of premium revenue per month.” VAN DER KOLK commented, “that’s extremely valuable information to decide whether a rewards participant should get paid or not.” ORTMANN replied, “basically, all the Vietnamese guys are gems” and “if [VF] knew how much money he brings us, he would probably not be content with a few \$1500 redemptions per month :)” ORTMANN also said, “as long as the total amount we pay out to him is reasonable, it’s fine” and “we must keep him motivated.” In addition, ORTMANN said, “well, I can only say – the Vietnamese guys deserve it, and shortly before xmas, it’s a great motivation boost.”

*Inferences:* Growth was driven by the content of paid uploaders and the traffic to their content was easily ascertained. The infringing nature of their content could also have been readily checked.

[108] Paragraph [106g]:

On or about December 2, 2007, via Skype, VAN DER KOLK told ORTMANN, “the idea behind the rewards should be that we attract new users / traffic to our sites, not pay for existing traffic / users IMHO.” The acronym “IMHO” generally means “in my humble opinion.” ORTMANN responded, “huge uploaders should profit, even if they have been with us for a long time.”

*Inference:* It was considered important to cultivate “huge uploaders”. This was not cyberlocker activity but mass distribution of illicit content.

[109] Paragraph [106i]:

On or about January 18, 2008, via Skype, DOTCOM asked ORTMANN, in German, “and I need to know exactly how much we pay monthly to uploader rewards.” ORTMANN responded, “the first rewards payment after Christmas was 76K.” DOTCOM replied, “maaaddnnneess!” and then he said, “no wonder we’re growing like that now.” In addition, DOTCOM said, “have growth” “not because of gigs” but “because of PAYMENT!” ORTMANN commented, “the payment came after the growth :)” and DOTCOM responded, “since the special people uploaded and promoted more.” ORTMANN agreed, “yes, that is surely relevant.” DOTCOM then said, “growth has less to do with the many gigs than with the rewards. in my opinion.” The term “gigs” refers to Gigabytes, a unit of measuring data-storage and file-size capacity.

*Inference:* Paid uploaders who distributed access to their content were driving growth.

[110] Paragraph [106j]:

On or about January 25, 2008, via Skype, VAN DER KOLK and ORTMANN discussed a particular repeat infringer and unindicted conspirator (herein referred to as "JH" ). VAN DER KOLK said, "his 500 and 1500 USD redemptions were disqualified" and "he has 6 \$100 redemptions pending." ORTMANN said, "he probably has 100% fraudulent files in his account." VAN DER KOLK responded, "most likely," "that's the big flaw in the rewards program" — "we are making profit of more than 90% infringing files," "so either we should just lower the points a bit and pay everybody, or stop paying rewards." VAN DER KOLK then said, "I assume with this rewards payment Kim wants to be very generous?" ORTMANN responded, "yes, but only for those users that brought premium sales :)"

*Inference:* The rewards programme generated subscription purchases because of the appeal of copyright material.

[111] Paragraph [106k]:

On or about January 26, 2008, via Skype, VAN DER KOLK sent ORTMANN a conversation between VAN DER KOLK and DOTCOM. During that conversation, VAN DER KOLK sent DOTCOM the rewards payments for a 2.5-week period. DOTCOM responded, "cool! "let's fucking pay." VAN DER KOLK replied, "okay I be less restrictive, fine with me :)" and DOTCOM responded, "good." DOTCOM also said, "*this is our growth motor,*" "you will see."

*Inference:* The content of paid uploaders drove business growth.

[112] Paragraph [106o]:

On or about July 15, 2008, via Skype, ORTMANN and VAN DER KOLK discussed a recent reward payment of "41.1K." VAN DER KOLK commented that the amount was, "a lot of money, thats for sure," but ORTMANN responded, "yeah, but we need the growth now." VAN DER KOLK added, "next one will be less, new video reward participants will slowly get slided more & more."

*Inference:* The content of paid uploaders drove business growth.

[113] Paragraph [106v]:

On or about November 8, 2009, via Skype, VAN DER KOLK and ORTMANN discussed a rewards payment of \$175,600. VAN DER KOLK said, “it’s still very fine in relation to our costs / income / profit if you think about it,” because “these users are making it happen.” ORTMANN asked VAN DER KOLK about a particular repeat infringer and unindicted conspirator, referred to as LR in Paragraph 53 of the Record of the Case, “is that a big contributor,” and VAN DER KOLK responded, “more than 70M” video views.” ORTMANN replied, “not bad :)” VAN DER KOLK offered, “but we can skip him if you want :)” and ORTMANN replied, “nono :)” “70M video views are worth up to 150K.”

*Inference:* Paid uploaders drove growth, and traffic to their content could be ascertained. In the same way the copyright status of their content could have been ascertained also.

[114] Paragraph [108h]:

On or about January 25, 2008, via Skype, VAN DER KOLK told ORTMANN, “the rewards system will only really contribute to our growth if we stop pissing off users” and “so as long as we disqualify users for infringing files it is only counter productive and very costly in my opinion” “because growth is mainly based on infringement anyway :)” Then ORTMANN asked, “what if we modulate our tolerance according to sales triggered? :)” followed by, “(not a very honest thing to do, but economically viable).” VAN DER KOLK replied, “yes, that way we at least don’t disqualify any valuable users.” Then VAN DER KOLK asked, “but isn’t the amount of sales & amount of reward points per account per month pretty linear?” and ORTMANN answered, “no,” “so]me people generate sales, some don’t.” Then ORTMANN said, “[TH] is e.g. just ranked 12 by sales.”

*Inference:* Rewards claimants were studied to see how much income they generated, but there was no concern about their infringing content, which was the main factor in Mega’s growth.

[115] Paragraph [123a]:

On or about January 25, 2008, via Skype, ORTMANN told VAN DER KOLK, “user [AT] has sold 782 premium accounts since Dec 09,” commenting “not even a Vietnamese.” VAN DER KOLK responded, “wow!” ORTMANN then said, “he has 2 million reward points, used 1.3million.” ORTMANN then listed the top four registered users who caused other users to purchase premium accounts. A few minutes later, ORTMANN told DOTCOM, in German, “[AT] in 1 st place with 782 Sales.” During the same conversation, DOTCOM pointed out that the 3<sup>rd</sup> place user “has 2.3 million reward points and 4,000 files” and then asked, “did we not pay him?” ORTMANN responded, “he is #3 in top sales.” DOTCOM stated that “he wants his money” and directed ORTMANN, “by all means pay [him].”

*Inference:* The income brought by rewards claimants was individually assessed. The volume of traffic and the size of portfolios was not consistent with ‘cyberlocker’ storage and hosting of non-copyright user-generated content.

*Disqualification in practice*

[116] Paragraph [46e]:

On or about July 3, 2007, VAN DER KOLK sent an e-mail entitled "Reward payments" to ORTMANN. In the e-mail, VAN DER KOLK wrote: "Hi Mathias, Hereby the batch payment file for the rewards over the last 15 days. Total costs: 6200 USD. Two 1500 USD redemptions from famous Vietnamese users again. Other than that only one hundred dollar redemptions, mainly MU [Megaupload.com] users. I banned around 25% and caught some fraudsters as well. Time for sliders for MU & M(R)V I'd say . . . Bram." In the attached reward payment file, repeat infringer TH, discussed below, was among those listed as being entitled to a \$1,500 payment.

*Inference:* The content and activities of uploaders were scrutinised before payment.

[117] Paragraph 103h):

On or about July 2, 2007, via Skype, ORTMANN asked VAN DER KOLK, “maybe we can do a selective payment to keep the people happy?” ORTMANN clarified, “only pay non-copyrighted videos? :)” VAN DER KOLK responded, “that’s gonna be a very time consuming thing to manage.” VAN DER KOLK also stated, “This time, I’ll ban the obvious cases. But we have to think about the rewards and it’s future. It’s more dangerous on MRV to pay people for uploading copyrighted content.” The acronym “MRV” refers to the video streaming portion of Megarotic.com. Despite this conversation, members of the Mega Conspiracy continued to make reward payments to repeat infringers, who uploaded copyright infringing files, including “obvious cases.”

*Inference:* Payments were made for traffic that was known to involve infringing content.

[118] Paragraph [46f]:

On or about August 24, 2007, VAN DER KOLK sent an e-mail to ORTMANN entitled “Reward payments”. In the e-mail, VAN DER KOLK wrote “Hereby the rewards batch payment file. Total costs: \$12,800 USD. Lots of 1500 dollar redemptions from Vietnamese uploaders again ...” VAN DER KOLK also wrote “I checked every file / video portfolio; however let me know if it’s too much, then I’ll check who else we can disqualify for whatever reason”.

*Inference:* The content of rewards claimants was examined before payment.

[119] Paragraph [46g]:

On or about October 24, 2007, VAN DER KOLK sent an e-mail entitled “Rewards payment” to ORTMANN. In the e-mail, VAN DER KOLK wrote: “Hi Mathias, Hereby the reward batch payment file. I was a bit more strict now, but still the total amount is \$8900. It’s really too easy to make rewards with split archive files, and we should really implement the IP limitation per X files per day as soon as possible. Thanks! Bram.” The term “IP” appears to refer to “Internet Protocol” address. In the attached reward payment file, repeat infringer TH, discussed below, was among those listed as being entitled to a \$1,500 payment.

*Inference:* There was concern to limit the cost of rewards payments but no concern to ensure that traffic to infringing content was not rewarded.

[120] Paragraph [103r]:

On or about November 18, 2007, via Skype, VAN DER KOLK said to ORTMANN, “I am doing the rewards now, and those split files are really costly. I often see Vietnamese file portfolio’s with DVD iso’s split into 100+ pieces.” An “iso” is a type of file containing all the data from a disc. VAN DER KOLK then said, “But for now we’ll pay those Vietnamese file portfolio’s right?” And, “this will be expensive again :(“ ORTMANN responded, “it will not be cheap, but we need to fill 20 more gigs in two weeks.” VAN DER KOLK replied, “Yeah that’s true, but making some changes so that they make a little less money wouldn’t hurt.” And, “they will not stop uploading if they get paid less I think.” The term “gigs” refers to Gigabytes, a unit of measuring data-storage and file-size capacity

*Inference:* Reward claimants were paid for traffic to infringing content.

[121] Paragraph [106h]:

On or about December 17, 2007, via Skype, VAN DER KOLK asked ORTMANN, “What would you expect as an acceptable amount for payout this time? ORTMANN responded, “15K,” and VAN DER KOLK replied, “okay I’ll adjust strictness accordingly :)” ORTMANN commented, “good.”

*Inference:* User portfolios were examined, but with the objective of limiting the cost of rewards rather than curbing infringement of copyright.

[122] Paragraph [106m(1)]:



... VAN DER KOLK then said, “it will not be that harmful, but I think they will continue to upload anyway” because “we’re still the only adult tube site that pays.” He also said, “since we have the sliders and the new counting logic our growth has been unchanged.” ORTMANN commented, “I am glad to hear that.” Then VAN DER KOLK said, “and now we can be a bit more relaxed with the payments, we don’t always have to find a reason to disqualify in order to reduce the total amount we’re paying.”

[123] Paragraph [106m(2)]:

On or about April 16, 2008, via Skype, VAN DER KOLK sent ORTMANN an e-mail from a registered user thanking them for an Uploader Reward payment. VAN DER KOLK commented, “What he doesn’t know is that he has a slider and that his points go 5 times slower from now on, it’s really good this way now.” He added, “no need to disqualify anyone anymore.” ORTMANN agreed, “perfect.”

*Inference:* Disqualification was related to economising on rewards payments rather than concern about copyright. By imposing sliders, the economic incentive for disqualifications on any basis was removed.

[124] Paragraph [106t]:

On or about May 25, 2009, via Skype, VAN DER KOLK told ORTMANN, “Rewards payment file & Translator payment file sent!” Then VAN DER KOLK said, “317 different paypal addresses being paid,” “nicely spread.” ORTMANN responded, “good, looks like most are \$100 :)” and VAN DER KOLK replied, “yes, the sliders do their job very well” Then VAN DER KOLK said, “This should really boost our popularity,” “unlike paying just a few users tens of thousands.” Then ORTMANN said, “good, paying now...” “86.3k.” A few minutes later, VAN DER KOLK said, “it’s fine I’d say with our profit,” “giving away less than 10% is very acceptable.” ORTMANN responded, “yes,” “especially in a growth phase,” and VAN DER KOLK replied, “And we really hardly disqualify anyone, we just block fraud that’s it.” The term “fraud” appears to refer to the users’ attempts to defraud the Mega Sites.

[125] Paragraph [106u]:

On or about July 31, 2009, via Skype, VAN DER KOLK and ORTMANN discussed a rewards payment. VAN DER KOLK asked, “How much was it in total btw?” and ORTMANN answered, “179300.” VAN DER KOLK commented, “oh not even \_that\_ bad” “for two months” “with our amount of uploads / revenue.” ORTMANN responded, “yep, it’s really cheap overall,” and VAN DER KOLK replied, “and this is not with any disqualifications of bad portfolio’s.” ORTMANN responded, “yep!” and VAN DER KOLK replied, “should really boost growth, let’s see.”

*Inference:* The rewards scheme was conducted with a view to profit and with no serious concern about the traffic to infringing content.

*Examining content / payment for infringing material*

[126] Paragraph [46b]:

As stated in Paragraph 25(e) of the Record of the Case, on or about February 5, 2007, VAN DER KOLK sent an e-mail to ORTMANN entitled "reward payments." Attached to the e-mail was a text file listing the users whom VAN DER KOLK had selected for reward payments. The file contained the users' e-mail addresses, usernames, and amounts of reward payments for that time period. For one user, who had a proposed reward amount of \$100, VAN DER KOLK described the uploaded content as, "10+ Full popular DVD rips (split files), a few small porn movies, some software with keygenerators (warez)." The term "DVD rips" commonly refers to infringing copies of copyrighted motion pictures and television shows originally contained on commercial DVDs. The term "warez" commonly refers to infringing copies of copyrighted computer software. VAN DER KOLK described the uploaded content of another user, who also had a proposed reward amount of \$100, as "Popular DVD rips." [...].

*Inference:* Payments were knowingly made for copyright infringing content.

[127] Paragraph [46c]:

As stated in Paragraph 25(g) of the Record of the Case, on or about April 15, 2007, VAN DER KOLK sent an e-mail to ORTMANN entitled "reward batch payment." In the e-mail, VAN DER KOLK stated: "We saved more than half of the money. Most of the disqualifications were based on fraud (automated mass downloads). The other disqualifications had very obvious copyrighted files in their account portfolio, but I was rather flexible (considering we saved quite a lot on fraud already). Total cost: 5200 USD. Thanks for paying! :) ...

*Inference:* Copyright infringement was only punished to achieve economies. If the total cost of rewards was acceptable, payment would be made for infringing material.

[128] Paragraph [46d]:

On or about June 7, 2007, VAN DER KOLK sent an e-mail to ORTMANN and DOTCOM entitled "Reward batch payment file." In the e-mail, VAN DER KOLK wrote: Hi Mathias, Hereby the reward batch payment for the past 10 days:

- I caught one fraudster with three 100 USD redemptions.
- One 1500 USD redemption from our friend [TH].

- Two 1500 USD redemptions from MRV [Megarotic.com] users, with mainly Asian videos in their portfolio: [user portfolios redacted].

I think we should really consider implementing a "silent slider" for MRV reward points, I think it's a bit too easy now. I didn't add four 100 USD redemptions for [username redacted], a Belgian guy that uploads gay porn to MRV, he also e-mailed us that his PayPal is blocked and he wanted to use Google checkout. The rest is standard 100 USD redemptions Total costs: 5900 USD (which more than half is generated through MRV) Thanks for paying! Bram [...]

*Inference:* Portfolios were examined and payments made to a conspicuous repeat infringer (TH).

[129] Paragraph [25f]:

On or about February 21, 2007, Van der Kolk sent an e-mail to Ortmann entitled "2 reward payment files." Attached to the e-mail was a text file listing proposed reward amounts, which ranged from USD \$100 to USD \$500, the Megaupload.com username, and a description of the uploaded content. For one user, who had a proposed reward amount to USD \$300, Van der Kolk wrote, "30849 files, mainly Mp3z, some copyrighted but most of them have a very small number of downloads per file." The term "Mp3" refers to an audio or music file, and the term "Mp3z" commonly refers to copyrighted musical recordings. For other users, all of which were selected for reward payments of USD \$100 by the Mega Conspiracy, he wrote the following: "Our old famous number one on MU, still some illegal files but I think he deserves a payment"; "Loads of PDF files (looks like scanned magazines)"; "looks like Vietnamese DVD rips"; and "This user was paid last time has mainly split RAR files, however more than 50% deleted through abuse reports."

*Inference:* Portfolios were examined and payments made for traffic to copyright infringing files.

#### *Assisting Repeat Infringers*

[130] Paragraph [106q]:

On or about November 22, 2008, via Skype, ORTMANN and VAN DER KOLK discussed a technical issue that required playing a video. ORTMANN said, "I had to try three videos. downloadid of that file, only the third one wasn't removed yet :)" and VAN DER KOLK responded, "haha." ORTMANN then said, "the good thing is that reuploaded videos convert instantly," "nice for repeat infringers." VAN DER KOLK replied "yes," "especially nice with the Mega Manager," and ORTMANN responded, "yes! :)" During this time period, the Mega Conspiracy was converting user-uploaded videos into the Flash video format and reproducing them to facilitate distribution.

*Inference:* The operation of Mega sites was designed to facilitate infringement.

[131] Paragraph [103cc]:

On or about January 16, 2009, via Skype, VAN DER KOLK said to ORTMANN, “good thing I have implemented the name ‘Megavideo’ to be displayed for watching video files from a MU user on MV :)” followed by, “I was thinking there, we should not disclose MU usernames anywhere.” ORTMANN responded, “very good! :)” and VAN DER KOLK replied, “also for copyright issues etc.”

*Inference:* By design, copyright infringement was made harder to detect.

[132] Paragraph [106r]:

On or about March 13, 2009, via Skype, ORTMANN sent VAN DER KOLK a message submitted by a Mega user, which read: “hi. ummm... seems like when I upload videos in MU and use them on megavideo, the videos go to the user named ‘Anonymous’ not mine.. please help me.” VAN DER KOLK responded, “yes I did that on purpose” “Because otherwise we disclose MU usernames.” ORTMANN replied, “TRUE.” And VAN DER KOLK added, “Also not good for repeat infringement offenders.”

*Inference:* The identity of copyright infringers was deliberately concealed.

*Specified Repeat infringers not terminated*

[133] SROC 2 has two examples of repeat infringers whom Warner Brothers specifically identified and brought to the attention of Megavideo (“ZS” and “HO”). These users were not terminated, and continued to accumulate more takedown notices and receive further payments after the Warner Brothers’ complaints. Mr Batato arranged an advertising campaign for HO on Mega sites some months after Warner Brothers identified HO as a repeat infringer.<sup>10</sup>

*Inference:* Identified repeat infringers were not disciplined. By design, the limited searchability of Megavideo hindered detection of infringers by copyright owners.

*Suspension policy – failure to suspend*

[134] Paragraph [106n]:

---

<sup>10</sup> SROC 2 paras [126] (ZS) and [127] (HO) (ROC bundle pp 197-201).

On or about April 15, 2008, via Skype, VAN DER KOLK sent ORTMANN a portion of an e-mail sent by a representative of Warner Brothers Entertainment Inc. to the Mega Conspiracy at dmca@megavideo.com. The portion of the e-mail stated: The following user [USERNAME REDACTED] appears to have circumvented Megavideo. When you look at his profile he shows that he has uploaded only 7 videos to Megavideo. However, this is not accurate. This user is circumventing Megavideo by linking to infringing videos directly and not searchable via Megavideo. Since these television episodes below prove that user [USERNAME REDACTED] has hidden and marked his videos as private, content owners such as Warner Bros. are unable to search and find all infringing content. I would like to request that his account be suspended. Below is an example of infringing content found from the linking site for user [USERNAME REDACTED]. The full e-mail also included multiple URL links to copyright-infringing materials, including the copyrighted television programs Smallville and Terminator: Sarah Connor Chronicles. Attached to the e-mail were two photographs, the first depicting the user's profile on Megavideo.com, and the second depicting a copyright-infringing video of Smallville uploaded by the user. VAN DER KOLK commented via Skype to ORTMANN, "the copyright holders are also getting smarter, with screenshots and everything :)" ORTMANN responded, "wow :)" As of January 20, 2012, [USERNAME REDACTED]'s account was active.

*Inference:* Identified repeat infringers were not disciplined. By design, the limited searchability of Megavideo hindered detection of infringers by copyright owners.

[135] Paragraph [114d]:

An account controlled by MW was temporarily suspended only after MW's account was found to be accessing too many links to files on servers controlled by the Mega conspiracy at one time. On or about April 19, 2010, VAN DER KOLK sent an e-mail to MW. In this e-mail, VAN DER KOLK wrote:

Dear [NAME REDACTED], Your personal

Megaupload/Megavideo account was found to be accessing 7 files/videos from 5 different IP addresses at the same time. This indicates that:

- you are using IP anonymizing or "hiding" tools
- your ISP is redirecting you through multiple proxies,
- you are performing concurrent remote file fetching to several hosts,
- you used a link-sharing download tool such as "XunLei" or "QQ Xuanfeng",  
or
- your account leaked, e.g. through phishing, sniffing or password guessing attacks.

Despite having processed over 700 takedown requests by April 19, 2010, for URL links to infringing content created by MW, on or about April 20, 2010,

members of the Mega Conspiracy reactivated MW's account from its suspended status.

*Inference:* Fraud against Mega was policed but there was otherwise no concern to curb the activities of obvious repeat infringers.

[136] This is detailed in Paragraph [134e]:

On or about May 2, 2009, via Skype, ORTMANN told VAN DER KOLK, "the workload incurred by the account blocking is consuming excessive resources. I am now implementing a different approach: Autoblocking, autounblocking, with initially 4 hours of suspension, doubled upon every reoccurrence..." VAN DER KOLK responded, "thats a very smart approach!" A few hours later, ORTMANN said, "now unblocking all 11000 blocked users :)" and VAN DER KOLK responded, "wow!!"

*Inference:* No serious effort was made to curb users who infringed copyright.

#### *The Reward Scheme Ends*

[137] The uploader rewards programme ended in late June 2011. About three months later, Mr Dotcom emailed PayPal (which had been the conduit for cash payments under the programme). Paragraph [25j] continues this email:

Our legal team in the US is currently preparing to sue some of our competitors and expose their criminal activity. We like to give you a heads up and advice you not to work with sites that are known to pay uploaders for pirated content. They are damaging the image and the existence of the file hosting industry (see whats happening with the Protect IP act). Look at Fileserve.com, Videobb.com, Filesonic.com, Wupload.com, Uploadstation.com. These sites pay everyone (no matter if the files are pirated or not) and have NO repeat infringer policy. And they are using PAYPAL to pay infringers.

[138] Although Mr Dotcom described the payment of rewards for infringing content as "criminal activity", Mega had done exactly that for more than six years. It had also failed to terminate repeat infringers who were paid rewards despite being the target of intensive takedown activity.

*Inference:* The rewards scheme was known to be unlawful because it involved payments to users who uploaded copyright infringing material.

[139] The end of the rewards scheme needs to be seen in the context of other developments affecting Mega. Earlier in the month, the linking site kino.to had been taken down. Kino.to was:<sup>11</sup>

particularly popular in German-speaking countries, was linking site that indexed material stored on alleged cyberlockers, including the Mega Sites. In June of 2011, law enforcement in Germany, Spain, France, and The Netherlands arrested more than a dozen people involved in the operation of the website

[140] On 13 June 2011, shortly after the kino.to takedown:<sup>12</sup>

BATATO and a third-party discussed Kino.to being closed down by European law enforcement. BATATO wrote, "That was expected . . . They were crazy to run a hoster AND a referrer site AND pay people to upload stuff."

[141] Mega was a hoster and paid people "to upload stuff". The main point of distinction was kino's connection with a referrer site, but the continuation of a rewards scheme was thought dangerous in this environment. There was evidently a perception that kino.to and Mega were associated:<sup>13</sup>

On or about July 6, 2011, DOTCOM forwarded an online story from Spiegel.tv to Ortmann about the takedown of the linking site kino.to by law enforcement in Germany, and wrote, in German: "Possibly not fly to Germany?"

[142] Also on the same day:<sup>14</sup>

Batato sent an e-mail to Ortmann forwarding a string of e-mails in German from an advertising entity saying that a customer wants their campaigns on a Mega Site discontinued because of concerns related to the kino.to takedown.

[143] A month later:<sup>15</sup>

On or about August 8, 2011, via Skype, BATATO said to ORTMANN in German that what Kino.to did "was really super fraud. You can practically call it organized crime." ORTMANN responded, "Exactly. And we have to separate ourselves from that." BATATO agreed, "yes."

*Inference:* The rewards scheme was known to be unlawful.

---

<sup>11</sup> ROC para [39p] (ROC bundle p 41).

<sup>12</sup> SROC 4 para [155c] (ROC bundle p 261).

<sup>13</sup> ROC para [38u] (ROC bundle p 38).

<sup>14</sup> ROC para [39p] (ROC bundle p 41).

<sup>15</sup> SROC 4 para [155c] (ROC bundle p 261).

***Repeat Infringer Biographies – A selection of material***

[144] Several repeat infringers are examined in detail here. This is either because of the revealing dialogue associated with an individual, or because their case illuminates some feature of the rewards aspect of the copyright conspiracy.

***Repeat Infringer “TH”***

[145] The uploader TH is expected to give evidence that:

- (1) From 2006, he obtained copyright infringing files of Vietnamese content, uploaded them to his premium account on Megaupload, and advertised the corresponding URL link on linking sites, along with a poster for the movie or television programme.
- (2) He frequently checked the URL links to see whether any had been disabled. Some were, but the underlying files were not disabled. He was not notified that any of his files on Mega had been the subject of copyright infringement takedown requests. His premium account was never suspended.
- (3) In 2006, before he received his first rewards payment, he received an email from Megaupload.com advising that he would not be paid because he had uploaded an infringing file. He was unsure of the copyright status of the file but replied that Vietnamese artists do not have copyrights. He then received his payment.<sup>16</sup>

[146] Mega received 1,200 takedown requests for URL links to TH’s infringing content. Mr van der Kolk processed all of these. Those links generated 1.2 million downloads of copyright infringing files hosted on Mega-controlled servers. (This is not the total number of downloads generated by his content, but only the downloads accomplished via the links that were the subject of takedown notices.<sup>17</sup>

---

<sup>16</sup> SROC 2 para [108], SROC 1 para [62c], (ROC bundle pp 160-162, 90).

<sup>17</sup> SROC 1 para [62a] (ROC bundle p 89).



[147] Between 2006 and 2011, TH received 26 reward payments. These represented a total of more than \$50,000.<sup>18</sup>

[148] In the six month period between February and August 2008, TH created and distributed links that generated over 10 million downloads. More than 130 of those links were subject to takedown notices.<sup>19</sup>

[149] The extracts below are largely self-explanatory. They cover a period of less than two years from 2006-2008, during which Messrs Dotcom, Ortmann and van der Kolk closely followed TH's activities. TH communicated with [support@megaupload.com](mailto:support@megaupload.com). At the relevant times, emails to this address were automatically forwarded to these respondents.

[150] The messages illustrate a number of familiar themes. While hundreds of takedown notices were lodged against TH's content, he was repeatedly paid. The respondents studied the traffic generated by his content and calculated the income this would bring to Mega. The messages on 17 June 2007 show that active steps were taken to enhance TH's provision of infringing content – the server capacity allocated to his account was increased to accommodate his 30,000 files (almost 2.5 terabytes).

[151] Paragraph [62d]:

On or about December 7, 2006, TH sent an e-mail to support@megaupload.com entitled "Thanks to Megaupload," thanking Megaupload.com for a recent reward payment of \$1,000, based on having accumulated 1,000,000 reward points in his premium account. That same day, ORTMANN responded to support@megaupload.com, omitting TH, asking, "Wow, does he really have that many premium points? Anyway, he gets all those Nguyens scattered around the globe to sign up, so it's money well spent!" The following day, ORTMANN received from support@megaupload.com an e-mail stating, "Yes, the guy can almost convert his third 1 Million points to another 1000 bucks[.]"

[152] Paragraph [62e]:

On or about December 20, 2006, TH sent an e-mail to sugnort@megaupload.com entitled "The Last Note." TH complained that he had not received a \$1,000 reward payment based on having accumulated

---

<sup>18</sup> SROC 1 para [62a] (ROC bundle p 89).

<sup>19</sup> SROC 1 para [62a] (ROC bundle p 90).

1,000,000 reward points in his premium account. TH stated that if he was not paid "within 24 hours," then he would expose the payment failure on "over 100 Vietnamese websites in the world." He further stated, "I really do not care about your payment or not. I do not give you a chance to cheat millions of user and uploaders anymore." On or about December 21, 2006, DOTCOM responded to ORTMANN and VAN DER KOLK, omitting TH, writing, "This is the fifth e-mail from this guy. WHY THE [expletive redacted] DOES NOONE CARE?" That same day, ORTMANN replied to DOTCOM and VAN DER KOLK, writing, "We do care. Bram was about to give me the final confirmation that the payment is legit, and I am sending it now."

[153] Paragraph [62f]:

On or about January 5, 2007, TH sent an e-mail to support@megaupload.com, which was nearly identical to the December 20, 2006 e-mail he previously sent. On or about January 5, 2007, ORTMANN wrote to another member of the Mega Conspiracy, "Money sent ... with a total of over 11 million pageviews of the files in his account, he surely deserves it!"

[154] Paragraph [108c]:

On or about March 11, 2007, via Skype, DOTCOM asked ORTMANN, in German, "dude, can you give me the stats in connection of which user accounts have the most premium sales?" DOTCOM clarified, "I mean rewards users." DOTCOM then said, "which uploaders have caused the most premium sales with their files." Then DOTCOM stated, "I would like to know how much premium our [TH] has brought!"

*Inference:* Mr Dotcom acknowledges the revenue TH brings to Mega.

[155] Paragraph [108d]:

On or about March 15, 2007, via Skype, DOTCOM asked ORTMANN, in German, "can you tell me how many premium accounts dear [TH] brought us? ORTMANN responded, "the analysis will take approximately 2 hours, I'll work on that right away." The following day, via Skype, ORTMANN said to DOTCOM, "morning...so far [TH] has provided us: -18 Million Download-Pageviews -112257 USD Premium-Sales to users who have downloaded at least 15 of his files." DOTCOM responded, "112257???" ORTMANN then said, "yep, those are the global nguyens." "Nguyen" is a common Vietnamese surname.

*Inference:* Dotcom again inquires after the amount of premium subscriptions TH has brought to Mega.

[156] Paragraph [62k]:

On or about June 17, 2007, TH sent an e-mail to Support@megaupload.com entitled "File manager." TH wrote, "I would like to get the links in my File

Manager, but I can not see any links in my account. Please adjust the system as soon as possible. Thanks in advance." That same day, ORTMANN responded, "You currently have 30,000 files in your account, totaling almost 2.5 terabytes. As you know, we officially only allow 250 gigabytes of storage per premium account, and our infrastructure and file manager are designed and built around this limitation. We are amazed that your file manager has worked up to this point, actually! Anyway, we have strengthened our infrastructure to handle extreme accounts like yours. Let us know if you can see your files again."

Paragraph [108e]:

On about June 17, 2007, via Skype, ORTMANN said to VAN DER KOLK, "[TH] is currently occupying 2.5 terabytes of disk space, btw – 10 times his allowance :)". VAN DER KOLK responded, "amazing," "and he's making good money with that :-)". ORTMANN then commented, "he is one of our most important uploaders... I don't regret any of the dollars we send him every month." VAN DER KOLK replied, "yeah."

[157] Paragraph [108f]:

On or about June 18, 2007, via Skype, ORTMANN said to VAN DER KOLK, "...the 3000 dollars for [TH] and [VF] are really money well spent." VAN DER KOLK replied, "yeah that I do believe."

[158] Paragraph [108g]:

On or about August 31, 2007, via Skype, ORTMANN said to VAN DER KOLK, "we could make 50K/month with [TH's] uploads alone :)". ORTMANN then said, "good that I convinced Kim [DOTCOM] not to delete him back when he complained about not having been paid :)". VAN DER KOLK responded, "yeah I bet," and "yes definitely."

[159] Paragraph [108h]:

On or about January 25, 2008, via Skype, VAN DER KOLK told ORTMANN, "the rewards system will only really contribute to our growth if we stop pissing off users" and "so as long as we disqualify users for infringing files it is only counter productive and very costly in my opinion" "because growth is mainly based on infringement anyway :)". Then ORTMANN asked, "what if we modulate our tolerance according to sales triggered? :)" followed by, "(not a very honest thing to do, but economically viable)." VAN DER KOLK replied, "yes, that way we at least don't disqualify any valuable users." Then VAN DER KOLK asked, "but isn't the amount of sales & amount of reward points per account per month pretty linear?" and ORTMANN answered, "no," "some people generate sales, some don't." Then ORTMANN said, "[TH] is e.g. just ranked 12 by sales."

[160] Paragraph [62u]:

On or about March 2, 2008, TH sent an e-mail to support@megaupload.com entitled "Reward points." TH wrote, "Please adjust the system for reward points as soon as possible. Because Available Points do not increase to match with Total Downloads that increase every hours. This problem lasts for 2 weeks. Please make a fair thing for uploaders." The following day, DOTCOM responded to ORTMANN, omitting TH, writing in German that it should give them pause when their main uploader complains. ORTMANN replied to DOTCOM that same day, writing in German that a new Uploader Reward policy was causing TH to lose points, and that TH will need to try harder if he wants to continue earning as much as \$10,000 per month through the program.

[161] Paragraph [62w]:

On or about March 19, 2008, TH sent an e-mail to support@megaupload.com entitled "Reward Points." TH complained about a new Uploader Reward policy that was causing TH to lose points. TH stated that if the policy was not adjusted, then he would "post on over 120 websites and notify users to stop buying premium account[s] with Megaupload." On or about March 19, 2008, DOTCOM responded to TH, writing, "You and your friends are at most 1% of our traffic. So please don't overestimate your importance to us. We are thankful for your support of Megaupload in the past and I think we have always been fair to you." DOTCOM further wrote, "In the future you will also earn rewards for every premium customer that you bring to us."

[162] Paragraph [108i]:

On or about March 20, 2008, via Skype, VAN DER KOLK sent ORTMANN a Skype conversation between VAN DER KOLK and DOTCOM, in which DOTCOM said, "i just sent a mail to [TH]. Check if he will make any major changes to his accounts or if his stats are dropping significantly in the next few days." VAN DER KOLK responded, "alright clear." Later on March 20, 2008, via Skype, VAN DER KOLK asked ORTMANN, "Do you know what happened with [TH] ?" because "He didn't seem to have uploaded any files in the past three weeks anyway." VAN DER KOLK then suggested, "He didn't get that 10.000 USD payment perhaps?" ORTMANN responded, "he got at least one that he acknowledged." And VAN DER KOLK replied, "damn what waste of money then :)" Then ORTMANN said, "well, he did bring us good sales in the past, but we don't say 'thank you,' we motivate for the future :)" VAN DER KOLK agreed, "exactly."

[163] Paragraph [108j]:

On or about March 28, 2008, via Skype, VAN DER KOLK asked ORTMANN, "so [TH] stopped uploading because of the change of reward points?" ORTMANN responded, "yep," "that's the only real casualty." VAN DER KOLK replied, "oh well, he will soon create another account under a different name and continue to use Megaupload" because "we're still the only one that really pays I think" — "I have seen that often." ORTMANN then commented, "at least he didn't delete all of his files yet."

[164] Paragraph [108k]:

On or about November 21, 2008, via Skype, ORTMANN sent VAN DER KOLK an e-mail written by TH, in which he wrote, "I have not been receiving money for 9 months while I still work hard for Megaupload. I really need money now. Please reply this email as soon as possible to make me comfortable. So that, I continue working for Megaupload at this time." ORTMANN asked VAN DER KOLK, "is he really still uploading/redeeming?!" because "I thought he was gone." VAN DER KOLK responded, "let me check," and ORTMANN replied, "okay, will send him a reply."

[165] Paragraph [62x]:

On or about May 10, 2008, TH sent an e-mail to support@megaupload.com. TH wrote, "I just came back to USA, and now my 11) for downloading or uploading from USA. I would like to start working for you now. Would you please let me know when the renovation will be done and how the new rule is? Thanks[.]" On or about May 11, 2008, ORTMANN responded, "Welcome back! The renovation is still in progress, but we can offer you a manual adjustment of your earned points according to the new standard as a special exception. Please send us a request before every redemption you plan to make." On or about May 12, 2008, DOTCOM responded to ORTMANN, omitting TH, writing: "Juhu. [TH] is back :-)" The German word "juhu" means "yay" in English.

*Inferences:* Known repeat infringers were repeatedly paid and their distribution of access to infringing content was deliberately enhanced. The income brought by repeat infringers was carefully studied but no concern was paid to their use of infringing content, despite the ease with which this could have been checked.

*Repeat infringer "TE"*

[166] TE is expected to give evidence that:

- (i) He uploaded copyright video clips, chiefly to Megarotic or Megaporn, to obtain rewards payments. He was constantly involved in this activity.
- (ii) He had some disagreements with Mega, which resulted in several episodes of temporary suspension. These were not related to his infringing content and he was not warned or disciplined for uploading copyright material.<sup>20</sup>

---

<sup>20</sup> SROC 3 para [139] (ROC bundle p 238).

At least 275 takedown requests were lodged against URL links pointing to TE's content. In a period of just over a month in 2008, TE received two payments and created 222 URL links to infringing material, while 156 takedown requests referring to his content were processed. Between August 2007-October 2008, he received nearly \$50,000 in 28 payments.<sup>21</sup> In September 2008 he claimed to have more than 9,000 videos uploaded.<sup>22</sup> He told [support@megarotic.com](mailto:support@megarotic.com) that he put in "on average 8 to 10 solid hours a day downloading, editing and preparing videos for uploading."<sup>23</sup> This was clearly not "user-generated content", a fact that was clear from other evidence, including Mr van der Kolk's scrutiny of his videos.<sup>24</sup>

During one of his periods of suspension, Mr Ortmann asked if TE had "uploaded very, very bad stuff, or should I write him a merciful e-mail and unblock him?" Mr van der Kolk replied "Yeah, that's a known infringer, he was just uploading adult stuff on M[ega] V[ideo] and lots of copyrighted stuff to MRV [Megarotic] and also inappropriate stuff. But yeah he can be reactivated again."<sup>25</sup>

A "known infringer", responsible for uploading "lots of copyrighted stuff" could safely be allowed by Mega to continue his work. In November 2007, Mr Ortmann and Mr van der Kolk debated whether TE should be paid. Mr Ortmann thought his content was a "valuable contribution". It was resolved to pay him but reduce the amount, possibly on the pretext of his "shady past".<sup>26</sup>

Despite this knowledge of his activities, TE was admitted to a "white list" of "trusted users" in May 2008.<sup>27</sup> His uploads would therefore "become available instantly", bypassing any auditor process.<sup>28</sup>

---

<sup>21</sup> SROC 2 para [110b] (ROC bundle p 164).

<sup>22</sup> SROC 2 para [110b] (ROC bundle p 164).

<sup>23</sup> SROC 2 para [110ss] (ROC bundle p 170).

<sup>24</sup> For example, SROC 2 para [110rr] (ROC bundle p 170).

<sup>25</sup> SROC 2 para [110h] (ROC bundle p 165).

<sup>26</sup> SROC 2 para [110m] (ROC bundle p 166).

<sup>27</sup> SROC 2 para [110dd] (ROC bundle p 168).

In June 2008, Mr van der Kolk reprimanded TE for splitting his files. This exchanged is detailed at paragraph [110gg]:<sup>29</sup>

“Why are you still cutting your videos in parts while we have finally implemented a white list for you so that you can post full videos? You have to stop this immediately or we will remove you from the white list.” Users were “cutting” videos into parts to gain additional points through the Uploader Rewards program. Also on or about June 12, 2008, TE sent an email entitled “white list” to account@megarotic.com. In the e-mail, TE wrote: I know you don’t want me to split up video’s, but what about video’s that are 110mb. I know, just upload them, you don’t mind, do you! Well I do, because I’m doing this for the income and you know it. Porn doesn’t do a damn thing for me at my age. I’m trying to co-operate, but I didn’t appreciate with being threatened with being removed from the white list if I split up video’s anymore. If you want to take me off the white list, so be it. We both know that I am the largest uploader you have, and have produced the highest view count for you. If you want me to quit, just say so! My wife would wants me to also. It might take me forever to delete all “my” video’s, but I would.

- (iii) TE was clearly familiar with the terms of the rewards programmes.<sup>30</sup> His response on this occasion shows that the ostensible 100mb limit for qualifying videos was not applied to him. In fact, dividing his files (to enhance his download scores) was frowned upon. He had been placed on the white list to encourage him to post “full videos”.

[167] While TE was on the “white list” another user emailed the support address at Megavideo and identified an apparently infringing video in TE’s account. That video was not deleted and remained available on the site until January 2012.<sup>31</sup>

[168] Eventually, TE became disillusioned with his income from the rewards programme and set up his own “tube site”. He also began deleting his videos from Mega sites, whereupon Mr van der Kolk deactivated his account. TE complained that he had lost access to his videos and was not able to delete them. Mr Dotcom forwarded one of his emails to Mr van der Kolk with the instruction: “Do not turn

---

<sup>28</sup> SROC 2 paras [110dd[, [110jj] (ROC bundle pp 168, 169)

<sup>29</sup> (ROC bundle pp 168-169).

<sup>30</sup> See, for example, SROC 2 para [110uu] (ROC bundle p 171).

<sup>31</sup> SROC 2 para [110oo] (ROC bundle pp 169-170).

this idiot’s account back on. And don’t give him access to his videos”.<sup>32</sup> TE’s videos remained publicly available despite the deactivation of his account and the infringing works kept generating revenue for Mega.

*Inferences:* Known repeat infringers were paid for traffic to infringing content and their activities actively encouraged. The 100 MB limit, ostensibly a check on copyright abuse, was waived to allow infringement to occur.

*Repeat infringer “BM”*

[169] The biography of BM illustrates the deliberate ineffectiveness of Mega’s response to takedown requests and the ease with which multiple links could be created to the files hosted by Mega. In this example, BM has, on repeated occasions, created links to a software file that clearly infringed copyright. The status of the file was evident not only from the takedown notices but also the name of the file. It was downloaded 114,300 times despite the takedown requests.

[170] The following details are given in the SROC1 at paragraph [49]:

- (i) On 7 September BM created a URL link to an infringing copy of the computer software “The Sims 2”. (The file name included the name “The Sims 2”. The file name was also associated with a linking site featuring copyright infringing materials.)
- (ii) That link attracted 7,300 downloads before 17 December 2009, when Mr van der Kolk received a takedown request for the file. He disabled the link but did not remove the infringing content. Other links pointed to that content.
- (iii) Four days later, on 21 December 2009, BM created a further link to the infringing file, again listing the linking site in the description. This link attracted 27,000 downloads until 16 March 2010. On that day a representative of the copyright owner submitted a takedown request.

---

<sup>32</sup> SROC 2 para [110uu] (ROC bundle p 171).



On 17 March, Mr van der Kolk disabled the link but the file and other links pointing to it were not affected.

- (iv) Also on 17 March, BM created another link to the infringing file, again using the linking site in the description. There were more than 80,000 downloads through this link until 1 September 2010, when Mr van der Kolk processed another takedown notice, again leaving other links and the file intact.
- (v) Also on 1 September 2010, BM created a further link in the same manner. Mr van der Kolk disabled the link in response to a takedown request but did not delete the file or other links to it.
- (vi) On 1 July 2011 BM created a further link to the same infringing file. This was still active on 19 January 2012.
- (vii) In total, Mega received over 1,500 takedown requests for URL links created by BM. BM was never terminated.

*Inference:* Access to infringing files was deliberately preserved.

*Repeat infringer “DR”*

[171] The outline of DR’s uploading career has some typical features. His portfolio included obvious infringing material. At least 2,500 takedown notices were lodged against his content. That content generated 13.7m views of infringing video files. Over two years, he was paid \$4,100 in 29 reward payments. Between two payments made in 2009, he uploaded more than 70 URL links to infringing content and Mega received 110 takedown requests made against his content.<sup>33</sup>

[172] His biography is notable for several reasons. Paragraph 121c outlines how DR’s account was suspended in September 2008 “for uploading inappropriate files.<sup>34</sup>” He appealed to Mr van der Kolk who replied: “We decided to give you

---

<sup>33</sup> SROC 2 para [121b] (ROC bundle p 190).

<sup>34</sup> SROC 2 para [121c] (ROC bundle pp 190-191).

another chance. Use it!” DR then sought clarification of why his account had been suspended:

“... so what can’t I upload. Anime or just certain anime because most people like me because of the anime. And I get the most attention from that.”

VAN DER KOLK replied by stating “[You can’t upload] Anything violating Megavideo’s rules, very specifically adult material – that goes to Megarotic instead.”<sup>35</sup>

[173] From that date until the closure of Mega sites in January 2012, 1800 takedown notices were lodged against DR’s content.

[174] The applicant submits that:

- (1) DR continued to deal with anime. Mr Batato arranged two advertising campaigns for DR, which involved the promotion of anime content. This is apparent in the names of the campaigns listed in Mr Batato’s messages to DR. The first was entitled “WatchMyAnime” and the second “Animebayocom”.<sup>36</sup>
- (2) In an earlier discussion with Mr Ortmann, Mr Batato was told the site [www.animea.net](http://www.animea.net) was a ‘pirate download-link site for [anime]’. It’s not legal but it’s not forbidden for them to advertise with us...”<sup>37</sup>
- (3) Anime was a popular form of copyright infringing content on the Mega sites.<sup>38</sup>

*Inference:* Obvious repeat infringers were repeatedly paid.

*Repeat infringer “VK”*

[175] VK’s URL links were the subject of 1,100 takedown requests. His portfolio included copyright infringing content such as movies, television programmes and software. His account was never terminated.

<sup>35</sup> SROC 2 para [121c] (ROC bundle pp 190-191).

<sup>36</sup> SROC 2 para [121d] (ROC bundle pp 191-192).

<sup>37</sup> ROC para [130a] (ROC bundle p 203).

<sup>38</sup> ROC para [103b] explains that a single linking site was showing 40,000 anime videos on Mega (ROC bundle p 203).

[176] On 13 September 2007 Mr Ortmann and Mr van der Kolk discuss VK's account. This exchange is reproduced at paragraph [109d]:<sup>39</sup>

VAN DER KOLK, "does [VK] ever redeem his points? :)" VAN DER KOLK responded, "yes he does." ORTMANN asked, "how much total so far?" VAN DER KOLK responded, "600 USD" "during the past 2 months." ORTMANN then commented, "there must be a ton of illegal stuff in that account." VAN DER KOLK responded, "with 97.000 files for sure indeed, but I am not that strict with single 100 USD redemptions, especially not from such huge accounts."

[177] Mr Ortmann and Mr van der Kolk's exchange is continued at paragraph [109b]:<sup>40</sup>

VAN DER KOLK sent the URL link [www.ftp2share.com](http://www.ftp2share.com) to ORTMANN and asked, "ever heard of that? You can upload or fetch a file there and then it gets uploaded to 5 big oneclick hosters at the same time (including us)." VAN DER KOLK also said, "tested it and the upload got attached to a premium account." VAN DER KOLK then sent ORTMANN the premium account number for repeat infringer VK, together with the number of uploads associated with that account. Based on VAN DER KOLK's statements, repeat infringer VK created an online service that enabled users to upload a file to the website [ftp2share.com](http://ftp2share.com), which would then upload the file to multiple "hosters," including the Mega Sites. This type of service would have facilitated the widespread distribution of copyright-infringing works.

*Inference:* Obvious repeat infringers were repeatedly paid.

***Forcing Premium Membership and Private Financial Gain by Limiting Viewing Duration***

[178] Outlined is a simple technique by which Megavideo achieved explosive growth from 2008. Users of the site were enticed into purchasing subscriptions by the limit placed on the viewing time available to non-paying users. If users were drawn into watching a movie, but could not watch it to completion, they would be tempted to buy a subscription to overcome the viewing limit.

[179] Much of the discussion below concerned the identification of a "sweetspot", or the duration of viewing time that would optimise the rate of conversion to paid subscriber status – "that critical time to cash in".<sup>41</sup> If this was too liberal, the

---

<sup>39</sup> ROC bundle p 163.

<sup>40</sup> ROC bundle p 163.

<sup>41</sup> SROC 2 para [104n] (ROC bundle p 147).

incentive to convert might be lost. If too strict, it might injure the flow of traffic to the site.

[180] Several points clearly emerge from these exchanges:

- (i) The respondents were deliberately exploiting the popularity of commercial movies protected by copyright. For example, Mr Ortmann told Mr Dotcom: “Movies last 90 minutes. They’re interesting in the last 20 minutes... The sweet-spot attribute might completely have to do with the fact that movies heighten the suspense towards the end”.<sup>42</sup>
- (ii) This activity was concealed within a site that was “nicely non-searchable” - copyright owners could not find their movies by directly searching Megavideo.<sup>43</sup> Link access to hosted videos was obtainable through external linking sites.<sup>44</sup>
- (iii) Messrs Ortmann, van der Kolk and Dotcom were all involved in discussions about the exploitation of commercial movies. Dotcom was anxious that he was not left “in the dark” about the manipulation of viewing times.<sup>45</sup>
- (iv) The infringing status of the content that attracted this traffic was obvious to them. For instance, Mr van der Kolk worried: “Don’t you think copyright holders will now get extra pissed?”<sup>46</sup> In a Skype conversation about the “sweet-spot”, Mr Ortmann told Mr Dotcom: “... long, low bit-rate movies are rare (DVD rips are high quality)”.<sup>47</sup>
- (v) Using Google analytics, it was possible to calculate the frequency with which viewers moved from the limitation message to the “buy now” button.

---

<sup>42</sup> SROC 2 para [104o] (ROC bundle pp 147-148).

<sup>43</sup> SROC 2 para [104h] (ROC bundle p 146).

<sup>44</sup> See for example SROC 2 para [107a] (ROC bundle p 157).

<sup>45</sup> SROC 2 [104p] (ROC bundle p 148).

<sup>46</sup> SROC 2 para [104j] (ROC bundle pp 146-147).

<sup>47</sup> SROC 2 para [104o] (ROC bundle p 145).

[181] Exchanges between the respondents concerning limiting viewing times run from paragraphs [104a] to [104p].<sup>48</sup> These paragraphs are reproduced below:

- a. In September of 2008, the Mega conspirators began limiting how long users could watch videos on Megavideo.com. The time limitation was changed from between 60 to 90 minutes, sometimes on a daily basis. If users wanted to continue watching videos, they were required to pay for premium membership. These limitations were imposed in part through a new video player.
- b. On or about September 7, 2008, via Skype, ORTMANN told VAN DER KOLK, regarding the new Megavideo player, “All it has to do is limiting the bandwidth by MV”. He added “We can limit it hard if needed”. A few minutes later, VAN DER KOLK said “I am looking forward to the first 1M\$ profit/month”. And ORTMANN responded “You are looking at December or January, provided that the new player performs well”. VAN DER KOLK added “But especially the fact that the video will stop after XX minutes and then show a message will trigger sales I think” because “the users want to see the rest”. ORTMANN replied, “Yes the concept is absolutely ingenious”, “much more incentive to pay than MU”.
- c. On or about September 11, 2008, via Skype, ORTMANN told VAN DER KOLK “Many people just watch one 2-hour movie”, and then he asked “How many movies can you watch in a row without getting bored?” VAN DER KOLK replied “That’s true indeed, okay let’s see what the new or current player with video view limitations will do then”.
- d. On or about September 14, 2008, via Skype, ORTMANN told VAN DER KOLK “Imagine people being interrupted shortly before a movie ends”, and “the inclination to pay will be higher than on MU”. VAN DER KOLK responded, “Pretty good point” and “This can be the new way of making revenue for Hollywood one day again”.
- e. On or about September 26, 2008, via Skype, ORTMANN told VAN DER KOLK “If you want to do some testing, [particular Megavideo.com URL] is a longer movie, parameters: 3 minutes quota, then 10 minutes waiting time”. VAN DER KOLK asked “When will the movie stop?” because “It’s already playing more than 3 minutes”. ORTMANN said “Now” and VAN DER KOLK responded “Ah yes”, “Wow”, “Very NICE”. ORTMANN then said “Yep, and we can also start offering higher-quality encoding as an option and really become the Rapidshare of the movie scene”. In March 2012, a German appellate court upheld decisions finding that Rapidshare.com, a Swiss file-hosting website, could be held liable for publication of copyright-protected material by third-party users.

---

<sup>48</sup> ROC bundle pp 162-163.

- f. On or about September 27, 2008, via Skype, ORTMANN told VAN DER KOLK “We have about 120,000 IPs that watched more than 120 minutes in the past 12 hours”, “That’s our base squeezing potential”, “if 1% pays...” “every day...”. VAN DER KOLK responded “That’s a lot of money indeed”. ORTMANN also commented, “I think 120 minutes is way too generous...” The acronym “IP” refers to Internet Protocol address.
- g. On or about September 27, 2008, via Skype, ORTMANN said to VAN DER KOLK, although the site design is NEVER a decisive factor here – content is king”, and VAN DER KOLK responded “Yes”. The “content” available on the Mega Sites was overwhelmingly copyright-infringing material.
- h. On or about September 27, 2008, via Skype, ORTMANN told VAN DER KOLK “We did some things right”, “we allowed fraud for a long time, fuelling our growth”, “then we forced our own player, making us explode”, “and now we can capitalize on it”. VAN DER KOLK responded, “Yes”. ORTMANN then said “And again, “It’s nicely non-searchable... really nice” and he also said “Let’s become the Rapidshare of video”. In addition, ORTMANN said “Our strongest country (USA) isn’t even fully awake yet” and VAN DER KOLK responded “Indeed”.
- i. On or about September 27, 2008, via Skype, ORTMANN sent VAN DER KOLK the following e-mail, which was submitted by a Mega user: “I love Megavideo, but I received a strange message and was not allowed to finish watching a movie. The message I received said “You have watched 77 minutes of video today. Please wait 120 minutes, or click here to enjoy unlimited use of Megavideo”. And I did, cause of course I wanted to finish the movie I’d started. Let’s see it was routed through [www.watch-movies.net](http://www.watch-movies.net), maybe that’s got something to do with it. Anyway, when I clicked on that nothing happened”.
- j. On or about September 28, 2008, via Skype, VAN DER KOLK asked ORTMANN “Don’t you think copyright holders will now get extra pissed?” ORTMANN responded “They wouldn’t know” because “They probably don’t watch their own stuff for 60+ minutes”.
- k. On or about October 28, 2008, via Skype, ORTMANN told VAN DER KOLK “Limiting MV to less than 90 minutes really triggers the flow”, “Movie length”. VAN DER KOLK responded “Yes indeed” “But the more we limit the more we hurt our growth”.
- l. On or about November 20, 2008, via Skype, VAN DER KOLK told ORTMANN “Also recent MV payments on PayPal look good now” and then he asked “limitation was unchanged?” ORTMANN responded “limitation is now at 70 minutes”.
- m. On or about November 21, 2008, via Skype, VAN DER KOLK and ORTMANN discussed how many users decided to pay for premium membership due to the time limitations on watching videos. VAN DER

KOLK said “Interesting: MV had 3 89,3 50 uniques redirected to “/:c=premium@1=1” “vs 29,933 for MP”. The acronym “MV” refers to Megavideo.com, and the acronym “MP” refers to Megaporn.com. ORTMANN responded “That reflects the ratio between redirects sent quite accurately”, “roughly 1:10”. ORTMANN then commented “Now if MP also generated the same amount of sales...” “We would have 300 new subscriptions a day”. VAN DER KOLK said “I don’t get it” and ORTMANN responded “Perhaps people just go elsewhere”, because “porn is generic”, “movies are not”. VAN DER KOLK added “Yeah that’s true”.

- n. On or about November 21, 2008, via Skype, VAN DER KOLK and ORTMANN discussed the idea time limitations to maximize the number of users who decide to pay for premium membership. VAN DER KOLK said “We have to reach that critical point to cash in” and “Yes, but with MV people watch 90-120 minutes”. ORTMANN responded “Limits beyond 3 hours – no conversion, 2 hours – some conversion, 90 minutes – more conversion, 70 minutes –major conversion” and “There is a huge difference between 90 and 70 minutes there”. VAN DER KOLK then said “Let’s see how many % clicks on the buy now button from the MV premium limitation message” and “(this is very good btw, google analytics)”. ORTMANN added “Yes, seems so”.
- o. On or about November 23, 2008, via Skype, ORTMANN and DOTCOM discussed whether the time limitation should be 60 or 72 minutes to maximize the number of users who decide to pay for premium membership. The conversation was originally in German. DOTCOM said: “MV is continuing to grow” “even with limits” and ORTMANN responded “Right”. Later DOTCOM said “What I don’t understand is why we don’t do what we agreed on. 60 minutes playtime / 60 [minutes] waiting. I don’t understand that. Isn’t that what we agreed on?” ORTMANN responded “Psychologically, I think it’s better if people have to wait a little less than they are allowed to see in one go. We’ve more than reached the target-payment level. We’ve continued to grow with real 72 Minutes. With real 60 Minutes, we are headed into new territory”. ORTMANN also said “Movies last 90 minutes. They’re interesting in the last 20 minutes”. Later DOTCOM said “Okay. It would just be nice if something like that got explained to me once in awhile. Just don’t leave me in the dark. I had assumed 60 [minutes] here. Yesterday we said we would try it out for four days now WITHOUT screwing around. Instead, it’s 72 [minutes] now. And yesterday you had raised the limits for an hour again. That isn’t what was agreed on. But it’s no big deal. It would just be fair and proper if you would keep to agreements or at least clarify in advance any changes to agreements. I really wanted to see where the journey would lead with 60/60. And four days won’t hurt anybody. MV will keep growing”. ORTMANN responded “No problem. We had identified 60 inexact Minutes as a sweet-spot. That it’s 72 Minutes in reality – so much the better for the user. The sweet-spot attribute might completely have to do with the fact that movies heighten the suspense towards the end”. DOTCOM asked “But you yourself said that most so the movies with us are being uploaded in high bitrate?” and ORTMANN responded “Low bitrate movies were really twice as long sometimes before the

user got the message”, “But long, low bit-rate movies are rare (DVD rips are high quality).” In this context, the phrase “DVD rips” appears to refer to infringing copies of copyrighted DVDs.

- p. On or about December 30, 2008, via Skype, ORTMANN told DOTCOM, in German, “What led to the miraculous MU turnaround at the end of July, we don’t know. But the introduction of MV limitations was our most important, deterministic change in 2008”.

*Inference:* Free viewing limits were manipulated to exploit the appeal of infringing copyright commercial movies and increase the rate of subscription purchases.

*Cogent – the expedited mass distribution of infringing content*

[182] In parallel with the exploding demand for video content in 2008, Mega adjusted its server arrangements to cope better with simultaneous traffic to the most popular files.

[183] From at least as early as October 2008, Mega leased bandwidth from Cogent Communications. Cogent is one of the largest carriers of internet traffic worldwide, “a multinational internet hosting provider that is headquartered in Washington DC, United States”.<sup>49</sup> From December 2010, Mega leased some 36 servers from Cogent.

[184] The assignment of Mega files to Cogent is described in the evidence at paragraph [24c]<sup>50</sup> in this way:

The preliminary analysis further shows that the Mega-Conspiracy measured the throughput, or bandwidth, that files on the Mega Sites were consuming. Files that demanded higher throughput, which meant that more users were accessing those files simultaneously were stored on faster servers located in Washington DC.

[185] Paragraph [102f] further explains:<sup>51</sup>

Software written by the Mega Conspiracy reproduced the most popular files onto faster Mega-controlled servers owned by Cogent Communications. The software executed every 60 seconds on an infinite loop, checking whether the Cogent servers had enough free space to host additional popular files. If there was free space available, the software would download and reproduce the popular file from the Mega-controlled server where it was originally stored onto the faster Cogent server; the file also remained on the original server,

---

<sup>49</sup> ROC para 22q.

<sup>50</sup> ROC bundle pp 15-16.

<sup>51</sup> ROC bundle pp 133-134.



resulting in multiple copies. The software measured popularity based on how much throughput, or bandwidth, was consumed by the file at that time. The software also removed files from the Cogent servers when the software determined that those files were not being distributed as frequently.

[186] Given the context of (among other things):

- (i) The high volumes of takedown requests directed at Mega-hosted files;
- (ii) Use of the rewards programme to encourage uploads of infringing content;
- (iii) The manipulation of viewing time to capitalise on the demand for commercial movies;
- (iv) The flow of traffic to Mega sites from linking sites cataloguing pirated content;
- (v) Personal knowledge that Mega's most popular content infringed copyright; and
- (vi) Admissions that Mega was in essence a pirate business.

It is clear that the Cogent initiative reflected a deliberate decision to further enhance access to infringing material. The most popular content, which would be assigned to this enhanced distribution system, would inevitably be commercial, copyright-protected material.

[187] The point made immediately above is confirmed by analysis of two Cogent servers leased by Mega. Paragraphs [72c]-[72d]<sup>52</sup> explain:

- (i) These servers contained 2,444 files.
- (ii) At least 90% of those files infringe copyright.
- (iii) A further 7% are pornographic videos (many of which are also copyrighted).

---

<sup>52</sup> ROC bundle pp 102–103.

- (iv) The remaining 3% cannot be assigned a copyright status because they are only a file fragment or have been encrypted.
- (v) More than one thousand of the files (approximately 43%) already had at least one takedown notice alerting Mega to the fact that they infringed copyright. More than 800 of those files had more than one takedown notice filed against their associated URL links. More than one hundred of those files had over 50 takedown notices submitted.
- (vi) Access to files affected by takedown requests was preserved by the existence of multiple links pointing to the file – with fewer than 244 exceptions, multiple links pointed to each file. (550 files had more than 100 URL links pointing to them; 100 files had more than 500 links).

[188] Paragraph [72a] suggests the very reasonable conclusion that:<sup>53</sup>

These faster servers thus facilitated the mass distribution of popular copyright-infringing works, which is incompatible with the notion that Megaupload.com was merely a cyberlocker, or that users were primarily interested in sharing personal, non-infringing materials. The establishment of these faster servers demonstrates that the Mega Conspiracy monitored the contents of the Mega Sites, analyzed user demand, and responded so as to maximize their financial profit.

[189] Mr Dotcom personally negotiated the contractual arrangements with Cogent. He and Mr Ortmann were alive to the significance of the Cogent system in Mega's architecture. At paragraph [148b]<sup>54</sup> Mr Ortmann observed to Mr Dotcom:

"if a US-court prohibits Cogent from providing us service, we will soon lose the vast majority of our connectivity worldwide."

[190] This remark was made in a conversation set out above, during which two men discussed ways to make Mega "invulnerable" to legal action. It shows that Cogent was central to Mega's distribution network – most of Mega's "connectivity" to its user audience depended on traffic to the highly popular content redirected to Cogent servers, from which simultaneous demand could be serviced. Demand of that kind was certainly related to copyright infringement.

---

<sup>53</sup> ROC bundle pp 102-103.

<sup>54</sup> ROC bundle p 102.

*Inference:* Mega deliberately increased its capacity to provide mass access to copyright-infringing files.

*Sources of traffic, linking sites and infringement*

[191] The following is a set of summary points on traffic, linking sites and infringement:

- (i) A URL link posted on a third party linking site, or anywhere else on the internet, makes the file it points to publicly accessible. This is inconsistent with any concept of private storage of data.<sup>55</sup>
- (ii) If the file is protected by copyright, this publication of the means of access is an act of infringement or at least facilitates one.
- (iii) Traffic flowing through linking sites to copyright files hosted by Mega enabled copyright in those files to be infringed by viewing or downloading.
- (iv) Mega's reward scheme created an incentive for links to infringing files of popular content to be posted on linking sites.<sup>56</sup>
- (v) Linking sites often catalogued infringing content available on Mega sites. They enabled Mega's holdings to be searched in a manner that was, by design, not possible by direct examination of the Mega sites.
- (vi) The respondents knew that the bulk of Mega's traffic flowed to its sites from linking sites. They examined this flow through tracking services such as Google Analytics and Extreme Tracking.
- (vii) The takedown of linking sites as a result of legal action was known to have an effect on traffic to Mega.

---

<sup>55</sup> SROC 1 para [74a] (ROC bundle p 104-105).

<sup>56</sup> ROC para [33a] (ROC bundle pp 26-27).

- (viii) The respondents knew about the indexing function of linking sites. They knew that users obtained access to copyright material, hosted on Mega sites, through URL links posted on linking sites.
- (ix) They also measured subscription purchases attributable to the traffic from particular linking sites.
- (x) They knowingly allowed linking or “warez” or “obviously stolen content sites” to advertise on Mega sites.

### *Terminology*

[192] The term “referrer site” may capture any site that enables internet content to be identified. Google is an obvious example. The applicant’s evidence uses the term “linking site” to denote a subset category, i.e. sites that specialised in referrals to infringing content.

[193] This specialisation was often notorious (e.g. Kino.to, the takedown of which caused concern about Ortmann travelling to Germany)<sup>57</sup> and sometimes reflected in the name of the linking site, e.g. “watch-movies.net”, [www.thepiratecity.org](http://www.thepiratecity.org), “seriesyonkis” and “animefreak”.<sup>58</sup> Some specialised in Mega content, e.g. [www.mulinks\[megaupload links\].com](http://www.mulinks[megaupload links].com), Megaupload.net, megauploadforum.net and megarelease.net. This is confirmed by the undercover inquiries of Agent Poston, explained at paragraph [40d]:<sup>59</sup>

In an undercover capacity, Agent Poston visited the following third-party linking sites: ninjavidio.net, megaupload.net, megarelease.net, kino.to, alluc.org, peliculasyonkis.com, seriesyonkis.com, surfthechannel.com, taringa.net, thepiratecity.org, and mulinks.com. All of these linking sites maintained an index of URL links to identified copies of copyrighted content that were stored on servers directly controlled by the Mega Conspiracy, and several of these websites exclusively offered Megaupload.com links.

*Inference:* Linking sites were the de facto indexes of infringing content on Mega. They provided the ‘private back end’ access to such content.

<sup>57</sup> ROC para [38u] (ROC bundle p 38).

<sup>58</sup> ROC para ‘14] (ROC bundle p 5).

<sup>59</sup> ROC bundle p 42.

[194] The ROC refers to the existence of thousands of linking sites.<sup>60</sup> Mr Ortmann said “We have a ton of parasitic domains”.<sup>61</sup> Some were sufficiently large to generate their own income streams and all linking sites had the potential to provide uploader rewards revenue to those who obtained links to the Mega sites. Others provided URL links to infringing content as a gratuitous service.<sup>62</sup>

[195] The respondents spoke about “referrer” sites and “our referrer sites” when discussion sites that would fall within the US concept of “linking sites”.

*Knowledge that Linking Sites were the conduit for traffic to infringing content hosted by Mega*

[196] Paragraph [331]:<sup>63</sup>

On or about September 17, 2011, Van der Kolk sent an e-mail to Ortmann, attaching a Google Analytics report on referrals to Megaupload.com from the linking site Taringa.net. The single page report indicates that, between August 17, 2010, and September 16, 2011, Taringa.net provided more than 72 million referrals to Megaupload.com, with the top 10 links including copyrighted software and music titles. The page indicates, for example, that the linking site produced 164,214 visits to Megaupload.com for a download of the copyrighted CD/DVD burning software package Nero Suite 10. This software program had a suggested retail price of \$99.

*Inference:* Piracy linking sites contributed traffic to infringing content hosted on Mega sites and known to the respondents who received reports.

[197] In early February of 2009, members of Mega discussed the third-party linking site watch-movies.net. This exchange is reproduced from Paragraph [130d 1]:

On or about February 1, 2009, via Skype, ORTMANN told VAN DER KOLK, “watch-movies.net seems to be offline,” then later, “it seems that their DNS provider is down.” VAN DER KOLK responded, “okay, probably not being taken down then,” and ORTMANN replied, “no,” and VAN DER KOLK replied “good :)” The next day, ORTMANN told VAN DER KOLK, “watchmovies. net’s problems are causing quite a few support requests: ‘Please cancel and credit back to the same card. The site is not responding anymore.’ ” VAN DER KOLK responded, “that’s not so cool...”

<sup>60</sup> ROC para [33a] (ROC bundle p 26-27).

<sup>61</sup> SROC 2 para [103v] (ROC bundle p 138).

<sup>62</sup> SROC 2 para [103v] (ROC bundle p 138).

<sup>63</sup> (ROC bundle p 28).

*Inference:* Traffic is known to flow from a linking site that is a target for takedown action.

[198] Paragraph [130d 1] (sic)

On or about February 2, 2009, via Skype, VAN DER KOLK told ORTMANN, “so the copyright holders target the spreaders as well now, not us which is good :)” ORTMANN responded, “they always do,” “it’s the sites providing search results that are targeted.” VAN DER KOLK replied, “we’ll be fine,” “where one site closes, 100 new ones will come up,” “as long as they don’t file a lawsuit against us everything will be just fine.”

*Inference:* The group knew that unlawful sites provided traffic to Mega.

[199] Paragraph [130d 3]:

On or about February 3, 2009, via Skype, DOTCOM told ORTMANN, in German, “MV has 1 million less users on Extreme Tracking since the removal of watch-movies[.net]. But strangely, this has no effect on payments. Really funny.”

*Inference:* One linking sites was known to contribute significant traffic to Mega sites.

[200] Paragraph [130d 4]:

On or about February 8, 2009, via Skype, ORTMANN told VAN DER KOLK, “yeah, warner bros. seems to be emailing many hosters these days, but at least watch-movies.net is back as watchmovies-links.net :)” VAN DER KOLK responded, “ah really, amazing :)” “let the cat&mouse game continue!” He then said, “as long as there is Internet there will be piracy.”

*Inference:* Mega knowingly derived traffic from pirate sites.

[201] Paragraph [130d 5]:

On or about February 9, 2009, via Skype, VAN DER KOLK told ORTMANN “MV is growing again” and “ORTMANN replied “Ah, thanks to watch-movies[.net]”.

*Inference:* Mega knowingly derived traffic from pirate sites.

[202] Paragraph [130b]:

On or about September 27, 2008, via Skype, ORTMANN said to VAN DER KOLK “Truveo is finding a whopping 40,000 Anime videos hosted by us and loading them in a nicely upsized embedded player”. VAN DER KOLK responded “Wow” and ORTMANN then commented “In total, they have indexed 1084273 Megavideo videos”. At that time, Truveo.com was a video search engine.

*Inference:* Linking sites index infringing content hosted by Mega and offset the limited searchability of the sites themselves.

[203] Paragraph [130c]:

On or about September 28, 2008, via Skype, VAN DER KOLK sent ORTMANN a link to the third-party linking site [www.surfthechannel.com](http://www.surfthechannel.com), commenting “They have an alexa rank 669 and are full with MV links”. VAN DER KOLK then said “Ah yeah there are plenty of sites like that, and there will be 10 new ones”.

*Inference:* Linking sites display links to Megavideo content. Users have been posting links on third party sites.

[204] Paragraph [130f]:

On or about May 25, 2009, via Skype, ORTMANN sent to VAN DER KOLK the following e-mail exchange between ORTMANN and a Mega user:

“Mostly women open this kind of disputes on PayPal”:

From Buyer: [NAME REDACTED] on 24/05/2009 18:25 PDT.

“I was watching a download of Dexter (para 231 is copyrighted) the TV Show, which I thought was on Megavideo, and it stopped playing, and said to join to see the entire show. I joined nad paid \$9.99 for a month through PayPal, but I cannot find that episode (or any others) on Megavideo”. (I responded: Your premium membership is valid not only for Megavideo.com itself, but also for our streaming service on third party sites. Go back to the original site and continue watching”). “Thank you, I finally figured that out when I received the confirmation email ... sorry for the trouble! THANKS!” VAN DER KOLK responded “Haha damn” “but good”. And ORTMANN replied “Yeah, it’s not easy to figure out”. The “streaming service on third party sites” refers to the embedded video players operated by the Mega Conspiracy available on third-party linking sites.

*Inference:* Linking sites were known to provide access to infringing content.

[205] Paragraph [74c]:

On or about March 20, 2011, VAN DER KOLK forwarded an e-mail from an unindicted conspirator to a separate unindicted conspirator, both of whom were then employees of the Mega Sites. In the original e-mail, entitled “Downloading Movies Issue (Megavideo)”, the employee stated: Please note that we have been receiving inquiries regarding issues in download movies/videos from Megavideo. Premium customers would state that they would be directed to the Purchase Premium page at Megavideo (<http://www.megavideo.com/?c=premium>) once they click on “Download Original” even if they were already logged in to their premium account. We were able to recreate the problem the other night and here is what we found out. Downloading the movie directly from Megavideo does not redirect the user to the Premium Purchase page. However, if they accessed the movie/video from third-party sites (tested sites: Quicksilverscreen, Watchnewfilms, Surfthechannel) and clicked on “Download Original” they would be redirected to the said page. We propose that we advise the customers to access them through the Megavideo website first before attempting to download a specific movie or video to prevent this from happening. The websites Quicksilverscreen.com, Watchnewfilms.com, Surfthechannel.com are third-party linking sites.

*Inference:* Linking sites were known to provide access to infringing content.

[206] Paragraph [33j]:

On or about January 28, 2010, in an e-mail entitled “Activating old countries”, a user of a Mega Conspiracy site asked BATATO: “Where can we see full movies?” BATATO replied “You need to go to our referrer sites. Such as [www.thepiratecity.org](http://www.thepiratecity.org) or [www.ovguide.com](http://www.ovguide.com)[.] There are the movie and series links. You cannot find them by searching on MV directly. That would cause us a lot of trouble”.

*Inference:* Mega cannot index its infringing content because of the risk of legal action but this content is known to be available through linking sites.

[207] Paragraph [33e]:

On or about January 14, 2009. BATATO sent an e-mail message to a Megaupload.com advertiser saying “You can find your banner on the downloadpages of Megaupload.com. Just choose a link for example from this site: [www.mulinks.com](http://www.mulinks.com)...”

*Inference:* It was known that Mega was being used on a large scale by linking sites rather than individual users taking advantage of a cyberlocker service.

[208] Paragraph [33d]:



On or about November 23, 2008, DOTCOM received an e-mail from a Mega Site user entitled “video problems”. The e-mail described “I’ve been trying to watch Dexter episodes, but the sound doesn’t match up with the visual... I didn’t choose to use your site, you seem to dominate episodes 6 and 7 of Dexter on alluc[.org, a linking site”. DOTCOM forwarded the e-mail to ORTMANN and wrote “... on many forums people complain that our video / sound are not in sync... We need to solve this asap!” “Dexter” is a copyrighted television series on the premium cable channel Showtime.

*Inference:* It was expected that users would visit Mega to access infringing content. Examples of such use did not result in instructions to remove the content.

[209] Paragraph [22k]:

On or about December 10, 2010, DOTCOM forwarded a complaint from a user that “Megaakey is not working” to ORTMANN and VAN DER KOLK. In the forward, DOTCOM writes: “This doesn’t work yet? We are advertising it. Why is it not working?” In the user’s e-mail he complained that he installed Megaakey, which provides Mega Conspiracy advertising to users in exchange for premium access to Megaupload.com and Megavideo.com, and the user was still receiving a message about the “Megavideo time limit”. The e-mail included apparent screenshots of the user’s computer, which shows the linking site animefreak.tv being used to attempt to watch an episode of the copyrighted television series “Fruits Basket” on Megavideo.com

*Inference:* It was expected that users would visit Mega to access infringing content. Examples of such use did not result in instructions to remove the content.

[210] Paragraph [74d]:

On or about September 16, 2011, co-defendant Andrus NOMM (“NOMM”) sent an analysis of Megavideo.com to ORTMANN by e-mail. The analysis includes comments from users of the Mega Sties, including the following: “The search function for the site should also list full length videos. Currently, movies that do not have copyright infringements are also not being listed in the search”. The analysis further indicates: “Movies should also be available in Megavideo and not from third party websites only[.]” The phrase “third party websites” appears to refer to third-party linking sites.

*Inference:* It was known that users viewed movies on Mega by using linking sites to find copyright infringing versions.

[211] Paragraph [39p]:

On or about July 6, 2011, BATATO sent an e-mail to ORTMANN forwarding a string of e-mails in German from an advertising entity saying that a customer wants their campaigns on a Mega Site discontinued because of

concerns related to the kino.to takedown. The website kino.to, which was particularly popular in German-speaking countries, was a linking site that indexed material stored on alleged cyberlockers, including the Mega Sites. In June of 2011, law enforcement in Germany, Spain, France and The Netherlands arrested more than a dozen people involved in the operation of the website.

*Inference:* Linking sites with Mega were known to be unlawfully providing access to copyright infringing materials.

[212] Andrus Nomm confirmed that he “and each of the co-conspirators periodically discussed the fact that users often discovered copyright-infringing content stored on the Mega sites through third party linking sites.”<sup>64</sup>

*Conspirators Study Traffic from Linking Sites*

[213] Paragraphs [130e] and [130f]:

On or about May 7, 2009, via Skype, ORTMANN told VAN DER KOLK, “interesting analysis results... out of our 15 top referrers, 10 are in Spanish ... and combined, they generate roughly 15% of our gross revenue”. VAN DER KOLK responded “Quite significant” “And in line with what I saw in the Google Analytics referrers”. Then VAN DER KOLK asked “Are we going to create some stats page or something with this?” And ORTMANN responded “What I will automate is revenue per downloaded stats so that you can check the monetary value of a takedown request”. A few minutes later, ORTMANN sent VAN DER KOLK the following list of the 15 top third-party linking sites that had generated premium accounts on the Mega sites:

seriesyonkis.com 13697 (Spanish)

surfthechannel.com 12574 (English)

vagos.wamba.com 10117 (Spanish)

taringa.net 8493 (Spanish)

peliculasyonkis.com 6468 (Spanish)

mcanime.net 4335 (Spanish)

wawa-mania.eu 4126 (Spanish)

alloshowtv.com 3890 (French)

cinetube.es 2795 (Spanish)

monblog.ch 2791 (French)

---

<sup>64</sup> SROC 6 para [170m].

sdd-fanatico.blogspot.com 2733 (Spanish)

sharebee.com 2705 (generic)

pordescargadirecta.com 2561 (Spanish)

dospuntocerovision.com 2487 (Spanish)

seriesgringas.us 2451 (Spanish)

ORTMANN explained “The number is the number of active premium accounts in the past 5 days ... lots will visit multiple sites, but still major revenue (\$7 per month per account on average)”. VAN DER KOLK responded “Yes, these sites are quite significant value to us then indeed”.

On or about July 19, 2009, via Skype, ORTMANN told VAN DER KOLK, “I just fear the day when those ten Spanish sites that make up for 20% of our payments get busted: (VAN DER KOLK responded “Nah sites will come and go all the time, and ORTMANN replied “True”)

*Inference:* It was known that major streams of traffic were from unlawful linking sites providing access to infringing content hosted by Mega.

[214] Paragraphs [33f] and [35g]:

On or about May 7, 2009, Ortmann sent an e-mail in German to DOTCOM indicating the top referring or linking sites to Megaupload.com by Megaupload premium users. The linking sites included: .seriesyonkis.com, surfthechannel.com, sharebee.com, taringa.net, watchmovies-links.net, cinetube.es, and megauploadforum.net

On or about May 17, 2009, NOMM sent an e-mail to ORTMANN entitled “Competitor Links Report”. The e-mail indicated that the top third-party sites used to reach Megavideo.com content were seriesyonkis.com, peliculasyonkis.com, dos\_puntocerovision.com, cinetube.es, and surfthechannel.com, which are all linking sites.

[215] Paragraph [74e]:

According to internal e-mails and documents obtained from Google, members of the Mega Conspiracy, including DOTCOM and VAN DER KOLK, began accessing Google Analytics reports for Megavideo.com, Megaupload.com and Megaporn.com. The Google Analytics account was opened at least as early as November of 2008 under the name “TIM VESTOR”, which is an alias for DOTCOM. Google Analytics provides website measurement tools, such as the number of visits during a specified time period.

[216] Paragraphs [74e 1] and [74e 2] proceed to detail some of the results of these Google Analytics reports for Megavideo.com and Megaupload.

1. A particular Google Analytics report shows that between November 19, 2010, and February 18, 2011, Megavideo.com had roughly 1 billion visits. Less than 13% of these visits were “direct traffic” – meaning visits that were likely generated by the user having directly typed the URL link into the web browser or having bookmarked the URL link. More than 85% of the visits to Megavideo.com were from “referring sites”, meaning the user appears to have clicked a URL link on the referring site that directed the user to Megavideo.com. The top referring websites during that time period were third-party linking sites, such as seriesvonkis.com (more than 110 million referrals) and sidereel.com (more than 60 million referrals). The reports from Google Analytics for the following time periods reflect similar data: February 19, 2011 – May 18, 2011; May 19, 2011 – August 18, 2011; August 19, 2011 – October 27, 2011.

2. A particular Google Analytics report shows that between November 19, 2010, and February 18, 2011, Megavideo.com had roughly 1 billion visits. Less than 20% of these visits were “direct traffic”, and roughly 80% were from “referring sites”. The top referring websites during that time period were third-party linking sites, such as taringa.net (more than 50 million referrals), seriesvonkis.com (more than 25 million referrals), and multiupload.com (more than 20 million referrals). The reports from Google Analytics for the following time periods reflect similar data: February 19, 2011 – May 18, 2011; May 19, 2011 – August 18, 2011; August 19, 2011 – October 27, 2011.

[217] Paragraphs [149a]-[149c] further explain Dotcom’s use of tracking sites:

The US Attorney’s Office for the Eastern District of Virginia expects a representative of the FBI to testify to the following facts:

a. As described in Paragraph 132 of the Record of the Case, eXTReMe digital V.O.F (“Extreme Tracking”), a Dutch company, provides website measurement tools, such as the number of visits during a specified time period. These tools are available at the website ExtremeTracking.com. According to records provided by Extreme Tracking, as early as May of 2005, the Mega Conspiracy opened 4 separate analytics accounts under the name “KIMBLE”, which is an alias for DOTCOM. These analytics accounts tracked the websites Megavideo.com, Megaupload.com, Megaporn.com, and Sexuploader.com.

b. As described in Paragraph 132 of the Record of the Case, visitors searching for terms specific to copyrighted works were referred to the Mega Sites on a daily basis. The searches described in Paragraph 132 included searches done through Google.com, amongst other online search engines.

c. DOTCOM’s Internet browsing history revealed that he had visited the Extreme Tracking website at least approximately 100 times, including but not limited to September 25, 2011 and October 31, 2011. Extreme Tracking analytic reports showed that several of the websites that referred traffic to Megaupload.com and Megavideo.com provided specific links to copyright-infringing content. The September 25, 2011 analytic report, for example, showed that the link [egsoftwares.blogspot.com/2010/04/nbaballers-phenom-ps2.html](http://egsoftwares.blogspot.com/2010/04/nbaballers-phenom-ps2.html) referred traffic to Megaupload.com. This link appears to advertise the copyrighted video game “NBA Ballers Phenom” for the Sony PlayStation 2 video game

console. Another report on that same date showed that the link como-conocia-vuestramadre. Seriespepito.com/capitulos-quinta-temporada-5/capitulo-24-doppelganger/ referred traffic to Megavideo.com. This link, translated from Spanish, refers to the copyrighted television series “How I Met Your Mother”.

*Inference:* It was known that Mega relied on traffic, through linking sites, to infringing content. These sources of traffic were carefully studied. Users visiting Mega directly were a small percentage of its traffic.

[218] Paragraph [148g]:

Throughout the Mega Sites’ existence, the defendants discussed their knowledge of, and reliance on, specific third-party referrer websites. For instance, on or about September 16, 2011, via Skype, DOTCOM asked ORTMANN in German why the Mega Sites recently experienced a “sharp decline” in traffic. ORTMANN responded by discussing Megaupload’s third-party linking sites and explained “the only referrer with major movement is taringa – they cut from one day to the next 50%, although that was the beginning of May. All other referrers are unchanged ... I am currently with the uploader analysis – not every referrer shows up as a referrer, many no longer link directly.

*Inference:* It was known that the major flows of traffic were through linking sites.

*Traffic volumes from linking sites*

[219] Paragraph [131a]-[131b]:

The U.S. Attorney’s Office for the Eastern District of Virginia expects a representative of the FBI to testify to the following facts:

a. According to a preliminary view of the Mega Sites’ source code, the Mega Conspiracy searched third-party linking sites for URLs linking to the Mega Sites. For example, source code in the file “cuevana.php” was designed to search for URL links referring to Megaupload” and “serie” (the Spanish word for “series”) on the third-party linking site cuevana.tv. The search results were stored in the log files, which were created on or about December 14 and 15, 2011.

b. As of January 19, 2012, the Mega Conspiracy had created at least 36 log files for various third-party linking sites, including cuevana.tv and icefilms.info. These log files listed more than 5 million Megaupload.com URL links, roughly 85,000 of which were unique URL links – in other words, many of the URL links appeared in more than one log and appeared more than once on the third-party linking sites. According to a preliminary review of the Mega databases, the most popular URL links were to copyright-infringing materials, such as the copyrighted television programs The Simpsons, Dexter, Family Guy, The New Girl, and 2 Broke Girls, and copyrighted motion pictures such as The Change-Up and Contagion. More than 95% of these

URL links were uploaded by users with registered accounts on the Mega Sites, and many of these registered users uploaded multiple URL links found in the logs. Of the 10 registered users who uploaded the most URL links found in the logs, all 10 also had at least 500 copyright takedown notices associated with their account. And as of January 19, 2012, each of these 10 registered users were still active on the Mega Sites.

*Inference:* The role of linking sites in providing traffic to Mega was specifically studied. The infringing nature of the content and the uploader responsible could have been easily ascertained.

[220] Paragraphs [132a]-[132b 6]:

The U.S. Attorney's Office for the Eastern District of Virginia expects a representative of the FBI to testify to the following facts:

a. eXTReMe digital V.O.F. ("Extreme Tracking"), a Dutch company, provides website provides website measurement tools, such as the number of visits during a specified time period. These tools are available at the website ExtremeTracking.com. According to records provided by Extreme Tracking, as early as May of 2005, the Mega Conspiracy opened 4 separate analytics accounts under the name "KIMBLE", which is an alias for DOTCOM. These analytics accounts tracked the websites Megavideo.com, Megaupload.com, Megaporn.com, and Sexuploader.com.

b. Records obtained from Extreme Tracking s how that visitors searching for terms specific to copyrighted works were referred to the Mega Sites on a daily basis. For example:

1. Between approximately December 1, 2010, and January 31, 2012:

i. Over 43,000 unique visitors searching for the term "pokemon" were redirected to the site Megaupload.com. Pokemon is a media franchise owned by Nintendo featuring copyrighted videogames, cartoons, trading cards, toys and books.

ii. Over 32,000 unique visitors searching for the term "psp" were redirected to Megaupload.com. The acronym "psp" refers to the PlayStation Portable, a handheld videogame console sold by Sony.

iii. Over 74,000 unique visitors searching for the term "keygen" were referred to Megaupload.com. A key generator refers to a software program that bypasses the digital rights management of copyrighted software.

iv. Over 12,000 unique visitors searching for the term "twilight" were referred to Megavideo.com. The Twilight Saga is a series of copyrighted motion pictures based on copyrighted novels written by American author Stephenie Meyer.

2. On or about December 13, 2010, over 650 unique visitors searching for the term "dexter" were referred to MegauDexter is a copyrighted television series

on the premium cable channel Showtime. A new episode of Dexter, entitled “The Big One”, aired on or about December 12, 2010.

3. On or about December 25, 2010, over 1,300 unique visitors searching for the term “Gorillaz” were redirected to Megaupload.com. The Gorillaz are a British musical band. Their copyrighted album “The Fall” was released on December 20, 2010, as a digital download exclusive to members of the band’s fan club, and then in April of 2011 as a physical release. A 12-month subscription to the band’s fan club currently costs \$45.00.

4. On or about January 2, 2011, over 700 unique visitors searching for the terms “harry” and “potter” were referred to Megaupload.com. The copyrighted motion picture “Harry Potter and the Deathly Hallows: Part 1” was released in U.S. theatres on or about November 19, 2010.

5. On or about January 11, 2011, over 200 unique visitors searching for the term “photoshop” were referred to Megaupload.com. Photoshop is a copyrighted graphics editing programme developed and sold by Adobe Systems.

6. On or about May 8, 2011, over 350 unique visitors searching for the term “thor” were referred to Megavideo.com. The copyrighted motion picture “Thor” was released in U.S. theatres only two days earlier, on or about May 6, 2011.

c. Records obtained from Extreme Tracking show that a handful of thirdparty linking sites provided a substantial portion of internet traffic to the Mega Sites. For example:

1. Between approximately December 1, 2010, and January 19, 2012, 10 third-party linking sites referred over 700 million unique visitors to Megavideo.com, accounting for over 78% of the total referred visitors. Referred visitors are in contrast to those who visit directly by typing in the website address. The 10 third-party linking sites are: seriesyonkis.com, allour1.com, surfthechannel.com, taringa.net, watch-movies.net, pelicalasyonkis.com, tv-links.eu, italia-film.com, streamiz.com, and serialeonline.pl.

2. Between approximately December 1, 2010, and January 19, 2012, over 1 billion unique visitors were referred to Megaupload.com by third-party linking sites. Of those, 56% were referred by 7 third-party linking sites: cuevana.tv, allour1.com, taringa.net, watchmovies.net, icefilms.info, forum.downparadise.ws, and stremiz.com.

3. On or about March 13, 2011, over 3.3 million unique visitors were directed to Megavideo.com by all referring sites. Of these visitors, over 1.3 million were directed from seriesyonkis.com, over 600,000 were referred by allour1.com, and over 350,000 from pelicalasyonkis.com.

4. On or about September 25, 2011, over 1.4 million unique visitors were referred to Mgavideo.com from third-party linking sites such as seriesyonkis.com and tv-links.eu, and over 3.8 million unique visitors were referred to Megaupload.com from third-party linking sites such as cuevana.tv or icefilms.info.

5. On or about November 6, 2011, over 4.4 million unique visitors were referred to Megaupload.com by third-party linking sites. Of these visitors, 54% were referred by just 2 sites, cuevana.tv and icefilms.info.

d. Records obtained from Extreme Tracking show that copyright infringement was evident in the names of URL links found on third-party linking sites. For example:

1. On or about February 16, 2011, over 23,000 unique visitors were referred to Megavideo.com from the following URL link: italia-film.com/teofilms/5292-thevampire-diaries-il-diario-delvampiro.html, and another 26,000 unique visitors were referred to Megavideo.com from the following URL link: stream.myblog.it/archive/2010/05/20/thevampirediariesstreaming.htm. The Vampire Diaries is a copyrighted television series on The CW channel. New episodes of The Vampire Diaries aired on February 10, 2011, and on February 17, 2011.

2. On or about April 2, 2011, over 45,000 unique visitors were referred to Megavideo.com from the following URL link: italia-film.com/teofilms/2451-greys-anatomy.html, and another 11,000 unique visitors were referred to Megavideo.com from the following URL link: megastreaming.biz/2009/09/28-streaming-serie-tv-greys-anatomystagione-6. Grey's Anatomy is a copyrighted television series on ABC. A new episode of Grey's Anatomy, entitled "Song Beneath the Song", originally aired on or about March 31, 2011, only two days prior to the Extreme Tracking data.

*Inference:* Analysis of traffic revealed Mega's reliance on traffic to infringing content via third party linking sites.

*Allowing "obvio[u]sly stolen content sites" to advertise on Mega Sites*

[221] SROC 7 shows that Mr Batato sold Megaclick<sup>65</sup> advertising to sites hosted or linked to "warez" or obviously infringing content. Discussions in March and April of 2011 show that Mr Nomm and Mr Ortmann were apprehensive about this practice. Mr Ortmann considered it "suicidal for M[ega] V[ideo]."<sup>66</sup> It is apparent that Mr Batato saw nothing wrong with allowing such illegitimate sites to advertise on Mega sites. One such exchange concerned a site called JSC, which Mr Nomm considered was an "advertiser of full length movies" and a "warez movies site". He asked Mr Batato to discuss the issue with Mr Ortmann. Despite this conversation, JSC was permitted to continue advertising on Megaclick.<sup>67</sup>

<sup>65</sup> Megaclick was a pay-per-click advertising program owned and operated by the Mega conspiracy that permitted advertisers to place advertisements on the Mega sites: SROC 3 para [163e] (ROC bundle p 230).

<sup>66</sup> SROC 7 para [172b].

<sup>67</sup> SROC 7 paras [171b], [172a].



## **Link deletion vs removal of access to infringing files**

### **Introduction**

[222] On receipt of a takedown notice, the DMCA requires either the removal of the file itself or disabling access to an infringing file. The Copyright Act 1994 (New Zealand) imposes similar obligations, if liability for storing infringing material is to be avoided.<sup>68</sup>

[223] In response to takedown notification, Mega did not delete the file indicated by the infringing URL link. Nor did it take steps to block access to the file by disabling all links pointing to that file. It deleted the particular link or links that the copyright owner had managed to identify. A typical infringing file had numerous links point to it, and more could easily be created by repeated uploads of the identical file (a process alleged to be expedited by the Mega Manager programme).

[224] The allegations about takedown procedures are:

- (i) If Mega believed its response to takedown notices complied with the DMCA, there was no need to deceive copyright owners into thinking that an infringing file had been deleted, or that all access had otherwise been blocked. That such deceptions were practised is evidence of the conspiracy.<sup>69</sup> The respondents knew that if owners were told the truth about Mega's link deletion practices, they would take legal measures to protect their copyright interests.
- (ii) Simple database analysis would reveal users whose URL links were repeatedly the subject of takedown requests. Irrespective of what should happen to the file associated with those links, the failure to sanction infringers could not be justified. There could be no justification for deliberately paying rewards to repeat infringers, identifiable in the database by the number of takedown notices their links had attracted.

---

<sup>68</sup> Section 92C.

<sup>69</sup> See para [273] ff.

[225] There is evidence that the respondents deliberately exploited the proliferation of links as a means of assisting infringers and frustrating the removal efforts of copyright owners. For example, at paragraph [133b]<sup>70</sup> Mr van der Kolk and Mr Ortmann discuss multiple links to a single file.

On or about February 15, 2009, via Skype, VAN DER KOLK and ORTMANN discussed multiple Mega URLs pointing to the same file. VAN DER KOLK told ORTMANN “Kim [DOTCOM] was suggesting to maybe limit it up to 10 of the same files per user, he just thought that it could be useful for some users to upload the same file several times if they want to have easy backups against deletions, or spread different links on different forums”. ORTMANN responded “Yeah, could be useful then”. And VAN DER KOLK replied “We would provide a feature that would make it harder to control for copyright holders”.

*Inference:* The capacity to generate multiple links was consciously exploited to injure the interests of copyright owners.

*Agent Poston generates multiple links and tests takedown response*

[226] The process of creating multiple links to the file, and Mega’s response to a DMCA takedown notice, were tested by Agent Poston. This is detailed at paragraph [40e]:

In an undercover capacity, Agent Poston visited sidereel.com and searched for a particular episode of the American television program Modern Family, a copyrighted work originally released by the American Broadcasting Company. Sidereel.com listed approximately sixty distinct URLs corresponding to that particular episode, all of which were then labelled as being hosted on Megavideo.com. Agent Poston successfully viewed and downloaded fifty of the sixty copyright-infringing video files, all fifty of which were hosted on Megavideo.com. Multiple unique URLs linked to the same copyright-infringing video of that particular episode.

Paragraph [40f]:

In an undercover capacity, Agent Poston uploaded to Megaupload.com a copyrighted video that had been provided by the copyright owner, with the express authorization to upload the work. The upload took approximately thirty-five minutes. As described above, Megaupload.com associated this file with a unique URL link. Agent Poston uploaded additional copies of the same file, and Megaupload.com provided additional links, which resulted in multiple unique links to the same copyrighted video on servers operated by Megaupload.com. These additional uploads of the same extract file took only a few seconds. This confirms that Megaupload.com does not create a second

---

<sup>70</sup> (ROC bundle pp 209-210).

copy of the file, but instead creates new URL links to the original file. After uploading the files, the copyright owner submitted to Megaupload.com a DMCA takedown notice listing only a subset of the unique URL links provided. Agent Poston confirmed that Megaupload.com disabled the link identified in the takedown notice listing only a subset of the unique URL links provided. Agent Poston confirmed that Megaupload.com disabled the link identified in the takedown notice but not the infringing video file itself, as the remaining links continue to provide access to the video. Megaupload.com did not notify the copyright owner that there were other URL links associated with the same file, and Megaupload.com did not notify Agent Poston, in his undercover capacity as the uploader, that the links had been disabled based on a DMCA takedown notice.

*Inferences:* Mega's system facilitated the generation of multiple links. Access remained after takedown action (despite on this occasion the file having only one uploader).

*The 'justification' for deleting only identified links*

[227] The applicant alleges that Mega purports to justify its policy of limited link deletion by claiming that:

- (1) The law of some countries allow individuals to make a private back up copy of copyright music, video or other protected data which they have legitimately acquired.
- (2) Mega cannot judge the legal status of a particular upload or download transaction.
- (3) When a copyright owner serves a DMCA notice on Mega, only the specified link is removed because other links may provide access to the file for other legitimate parties. This is because when two or more users upload the same file (e.g. a DVD of 'Lord of the Rings'), Mega stored only one copy of the file. Someone's pirated DVD file may be another person's legitimate backup.

Mega allowed a situation in which traffic to a file could continue (via extant links) after "takedown" notification by a copyright owner.

[228] Paragraph [45b] the applicant says would refute the Mega justification:

The U.S. Attorney's Office for the Eastern District of Virginia expects a computer specialist with the Federal Bureau of Investigation ("FBI") to testify to the following facts:

a. Every digital file has a "fingerprint", which can be generated by applying a mathematical algorithm to the file. Though a variety of algorithms exist, a particular algorithm, known as Message-Digest 5 ("MD5"), produces an effectively unique 32-digit identification value, commonly called an "MD5 hash". Altering a file, for example by changing the length of the file, will change its MD5 hash. If two users, using the most prevalent techniques, each create a compressed digital back-up copy of the same motion picture DVD on different computers, the two back-up copies will have different MD5 hashes. Even if a single user creates two compressed digital back-up copies of the same motion picture DVD on the same computer, the two back-up copies will have different MD5 hashes because they were created at different times.

*Inference:* The unique fingerprint of a digital file means that there is no justification for preserving access to a file associated with an infringing URL link. If two users each upload the digital file of a DVD (e.g. "Lord of the Rings"), the Mega system would recognise these as different files and store both. Although they were both generated from the same commercial DVD, the different manner of their conversion to an uploaded digital file will mean they have different hash values.

[229] A situation in which an "innocent" user and an infringer both generate URL links pointing to the same file will not occur.

[230] The applicant alleges that this is further illustrated by paragraph [162] (especially subparagraph c). Mega sites hosted "numerous versions of the same copyrighted material". The film "Lord of the Rings: The Return of the King" is used as an example. Multiple versions of this film were hosted despite the similarity in the content available to users. This was because the Mega automated system recognised different uploads of the film as having a different MD5 hash. Two such versions each had a different hash and accounted for nearly 100,000 views. They were associated with multiple links (an indication of repeated uploads of the same unique file, though in these cases from different user accounts). Both were the subject of takedown notices.

[231] The applicant alleges that there was no justification for failing to delete these files for copyright infringement, or block all access to them, on the basis that to do so might affect some other legitimate or private version of "Lord of the Rings..." These

particular versions of the film were detected by the copyright owner on the internet and were plainly being distributed in a manner that infringed copyright. The circumstances are inconsistent with any notion of private backup or use. Deletion of these files would affect no other hosted version.

[232] Paragraph [167] looks at this issue from another perspective. It analyses the situation in which obvious infringing files had only been uploaded by one user. The alleged risk of deleting another user's file could not exist, yet Mega did nothing to block access on receipt of takedown notices.

### **The failure to remove infringing links**

#### **Introduction**

[233] The applicant alleges that on some occasions Mega not only failed to remove access to an infringing file, but failed to remove even links that were identified in takedown notices or other complaints made by copyright owners. It is alleged that Mega also tried to slow the rate of link deletion for copyright infringement to avoid reductions in traffic and revenue. They say Mega's response to complaints of infringement depended on the source of those complaints; they might be ignored if there seemed little likelihood of being sued.

#### *Mexico and Brazil*

[234] Paragraphs [38j], [76] and [133] concern the efforts of a body representing Mexican copyright owners (the Asociacion Protectora de Cine y Musica, or APCM) to protect copyright in their works.

[235] Paragraph [38j] explains that on 4 February 2009:

... [legal@megaupload.com](mailto:legal@megaupload.com) received an e-mail from a representative of various copyright owners, including Sony BMG Music Entertainment Mexico, Columbia Pictures Industries Inc, Disney Enterprises Inc, Paramount Pictures Corporation, Twentieth Century Fox Films Corporation, and Warner Bros. Entertainment Inc. In the e-mail, the representative stated that "infringing items are being offered [on the Mega sites] in a manner that is not authorized by our members or its agents, or the law". The representative went on to list over 6,000 URL links to copyright-infringing materials available on the Mega Sites.

[236] Paragraph [38j] continues, on or about 23 April 2009:

[legal@megaupload.com](mailto:legal@megaupload.com) received another e-mail from the same representative, listing over [1,000] 255 URL links to copyright-infringing materials available on the Mega Sites.

[237] On or around the same day of April 2009:

DOTCOM sent an e-mail message to VAN DER KOLK, ORTMANN and BENCKO in which he complained about the deletion of URL links in response to infringement notices from the copyright holders. In the message, DOTCOM stated: “I told you many times not to delete links that are reported in batches of thousands from insignificant sources. I would say that those infringing reports from MEXICO of ‘14,000’ links would fall into that category. And the fact that we lost significant revenue because of it justifies my reaction”.

[238] On or around the same day of April 2009, Mr Ortmann and Mr van der Kolk also discuss the Mexican takedown notices via Skype:<sup>71</sup>

ORTMANN told VAN DER KOLK “Maybe try undeleting them” and VAN DER KOLK asked “You want to risk that?” Then VAN DER KOLK said “I mean MX is just MX, we could ignore them”, and ORTMANN added “It’s not like Mexico is going to sue us in Hong Kong”. ORTMANN continued “Just for testing, we should undelete those files”, “for one day”, “we can excuse it as a tech glitch”. VAN DER KOLK added “I often ignore reports from certain countries, such as VN”. In this context, the abbreviations “MX” and “VN” appear to refer to Mexico and Vietnam, respectively.

[239] Paragraph [133c 2] continues:

Later that day, DOTCOM instructed ORTMANN, in German, “And please do what I wrote bram. Undelete everything that was in the last 4 weeks reported from non first world countries. SIMPLY everything. And you will see we have daily record again”.

*Inference:* Countries outside the “first world” contribute considerable traffic but do not present such a high risk of legal action.

[240] The correspondence between the respondents continues at paragraph [133c 3]:

Later that day, ORTMANN sent DOTCOM a portion of the APCM e-mail, which stated that APCM Mexico is the authorized representative of, amongst others, Columbia Pictures Industries, Inc., Disney Enterprises, Inc., Paramount

---

<sup>71</sup> SROC 2 para [133c 1] (ROC bundle p 210).

Pictures Corporation, and Warner Bros. Entertainment Inc. ORTMANN told DOTCOM, in German, "if true, Bram has not done anything wrong." A few minutes later, DOTCOM blamed the takedowns for causing "50k revenue gone."

[241] Paragraph [133c 4]:

Later that day, ORTMANN told BENCKO, "the takedown notices were legitimate for sure," "however, calculated risk could work here".

[242] Paragraph [133c 5] continues with more instruction from Mr Dotcom:

Later that day, DOTCOM told VAN DER KOLK and ORTMANN: make a list of all links that were reported from Mexico, Brazil, and other non first world countries in the last 4 weeks. and undelete all of them. They have not sent us legitimate takedown notices with sufficient proof that they represent the right holders for every single link. and from now on you will only delete links from the USA, France, Germany, UK and SPAIN instantly.

[243] Paragraph [76b] explains how:

Also on April 23, 2009, VAN DER KOLK forwarded to ORTMANN the APCM's February 4, 2009 e-mail, writing, "another candidate for undeletion." Minutes later, VAN DER KOLK forwarded to ORTMANN the APCM's April 23, 2009 e-mail, writing, "also needs to be undeleted." Based on these e-mails, it appears that access to the URL links identified by APCM had been disabled (although the underlying copyright-infringing materials remained accessible through other URL links pointing to the same materials), and that DOTCOM instructed VAN DER KOLK and ORTMANN to "undelete" the URL links, thus making them available to the general public.

[244] Paragraph [38k] also details Mr Dotcom's insistence on geographic priorities in link deletion:

On or about April 24, 2009, DOTCOM sent an e-mail to Bencko, Ortmann, and Van der Kolk indicating, "I remembered the steep drop of revenue at the same time in 2008 and thought that this might have also been caused by careless mass link deletions. This made me very mad, especially because I told you that such mass deletions should be prevented and sources checked much more carefully. I am sure such mass link deletions are also contributing to a drop of revenue ... In the future please do not delete thousands of links at ones from a single source unless it comes from a major organization in the US."

*Inferences:* Mass deletions of links identified by copyright owners result in a sudden loss of income. Mr Dotcom wants complaints checked more carefully to ascertain if takedown requests can be safely ignored. He directs a further tightening of the

policy; there will only be large-scale deletions if the complaint comes from a major US organization.

[245] On or around the same day in April 2009, Mr van der Kolk and Mr Ortmann continue discussing takedown notices from the Mexican authorities, at paragraph [133c 6]:

The following day, April 24, VAN DER KOLK told ORTMANN, “me deleting them is normal procedure, especially since we’re soon being sued. This was not sent from a Gmail or Yahoo address, this is the Mexican MPAA.”

[246] Mr Ortmann and Mr van der Kolk’s discussion continued later in April of 2009, at paragraph [133c 7]:

On or about April 27, 2009, VAN DER KOLK asked ORTMANN, “People are already re-sending their DMCA notices now, can I resume processing them again?” ORTMANN answered, “yes, first-world only.”

*Inferences:* This is the outcome of the policy. Copyright owners have immediately resent takedown notices because the URL links originally deleted have been restored. Mr van der Kolk is only to remove links if they originate in the “first-world”

[247] ACPM identified more than 7,000 URL links in February and April 2009. Paragraphs [76a]-[76c] explain that:

... As of January 19, 2012, approximately 4,600 of these 7,000 URL links to copyright-infringing materials were still active and available on the Mega Sites (roughly 2,400 URL links were disabled as a result of later copyright takedown notices; however, the copyright-infringing content remained accessible to members of the public).

Despite receiving the February 4 and April 23, 2009 takedown requests, the Mega Conspiracy not only failed to completely block access to the copyright-infringement content but purposefully chose to distribute these files after being told they were infringing because removing the content would have reduced their revenue. After these takedown requests were submitted, new URL links to the same infringing content were created, and the infringing content was downloaded more than 1.7 million times through the new, post-notice URL links.

In total, ACPM Mexico submitted at least 400 takedown requests, which identified more than 550,000 URL links to copyright-infringing materials available on the Mega Sites. ACPM Brazil submitted at least 2,500 takedown requests, which identified more than 1.2 million URL links to copyright infringing materials available on the Mega Sites.



*Inference:* The respondents thought there was less risk of being sued by commercial interests outside the ‘first world’. On that basis, even specifically identified links to infringing content were not deleted.

*India*

[248] Paragraph [133a]:

The U.S. Attorney’s Office for the Eastern District of Virginia expects a representative of the FBI to testify to the following facts: a. On or about December 26, 2008, via Skype, ORTMANN said to VAN DER KOLK, “wow, an Indian subpoena requesting MV uploader credentials...” VAN DER KOLK responded, “wow,” “ah that one from the police,” “I think I saw that one.” Later, VAN DER KOLK said, “it’s just Indian police,” and ORTMANN responded, “yes, we can probably ignore this one.” VAN DER KOLK suggested, “we can always say that we never received their e-mail,” and ORTMANN responded, “yep,” “but they probably also sent a postal letter (scanned attachments).” VAN DER KOLK replied, “ah yes then it’s a different story,” and then he asked, “do we get many physical mail these days for copyright issues?” ORTMANN responded “very few” and VAN DER KOLK commented “good”.

*Inference:* This example suggests an attitude to countries that are not thought to pose an immediate legal risk to Mega.

*Limits on link deletion*

[249] Paragraph [31d]:

On or about September 4, 2009, a representative of Warner Brothers Entertainment, Inc. (“Warner”), sent an e-mail to Megaupload.com, stating that Warner was “unable to remove links” to copyright-infringing content on Megaupload.com using the Abuse Tool. In the e-mail, the Warner representative requested an increase in Warner’s removal limit, which is controlled by the Mega Conspiracy. On or about September 8, the representative sent a follow-up request, and on or about September 9, the representative sent another follow-up request. On or about September 10, Ortmann sent an e-mail to DOTCOM, stating, “They are currently removing 2500 files per day - a cursory check indicates that it’s legit takedowns of content that they own appearing in public forums.” The term “public forums” likely refers to third-party linking sites. Ortmann also stated, “We should comply with their request - we can afford to be cooperative at current growth levels.” DOTCOM responded that the limit should be increased to 5,000 per day, but “not unlimited”, demonstrating that the Mega Conspiracy arbitrarily limited the ability of copyright owners to remove infringing content from the Mega Sites.

*Inference:* An arbitrary limit was placed on the ‘legitimate’ takedown of links to infringing content, which Warner Bros. had identified on linking sites.

*Hindering the actions of an infringement detection agency*

[250] Paragraph [133d]:

On or about May 20, 2009, via Skype, ORTMANN told VAN DER KOLK, “DtecNet is getting more annoying. Kim [DOTCOM] requests to ignore their notices until Sunday evening.” VAN DER KOLK replied, “okay.” As discussed in Paragraph 93 of the Record of the Case, a number of copyright owners hired DtecNet, also known as MarkMonitor, to identify infringing copies of copyrighted works that were publicly available on the Internet, including through the Mega Sites.

*Inference:* The respondents hindered attempts to curb infringement.

[251] Paragraph [133e]:

On or about June 2, 2009, via Skype, ORTMANN told VAN DER KOLK, “I will give you the HD showcase videos shortly, and we don’t want DtecNet or anybody else to interfere with that.” VAN DER KOLK responded, “ah right, we can introduce a white-list table easily.”

*Inference:* The respondents knowingly displayed copyright infringing material and tried to defeat the efforts of copyright owners to protect their interests.

*Manga*

[252] Paragraph [103ss]:

Later that day, VAN DER KOLK told ORTMANN, “We also often get DMCA notices for the manga,” “funimation, a US company is often sending us huge batches.” ORTMANN responded, “I told Kim [DOTCOM] that Manga is commercial stuff, too, and he said that the Manga companies are tiny and will never sue (?).” VAN DER KOLK replied, “I don’t think so, that’s quite a big business also,” and ORTMANN said, “I think so as well.”...

*Inference:* The respondents flouted the rights of copyright owners if they thought there was little exposure to legal action.

*Preventing the loss of files from link deletion*

[253] Paragraph [39b]:

On or about February 13, 2007, Ortmann sent an e-mail to Van der Kolk entitled "my concerns about the thumbnails table." In the e-mail, Ortmann asked Van der Kolk to create "a dummy lifetime premium user," stating that "[t]his is very important to prevent the loss of source files due to expiration or abuse reports."

*Inference:* The respondents deliberately hindered the efforts of copyright owners to protect their property rights.

## **The Deception of Copyright Owners**

### ***The Abuse Tool and Takedown Notice Deceptions***

[254] Paragraphs [34] and [80]-[96] describe a number of occasions on which Mega falsely assured copyright owners or their agents that:

- (1) Files or content had been removed in response to specific takedown notices, or
- (2) The Abuse Tool deleted files (rather than merely the link submitted to the Tool), or
- (3) Mega's policy was to delete material upon notification and it had procedures to detect copyright violation.

[255] The misrepresentations caused the owners identified in the table to continue submitting notices rather than taking other action against Mega.<sup>72</sup>

### ***The Deception of Paypal by Mathias Ortmann***

[256] Paypal was the online payment company through which Mega chiefly received its income. Paypal conveyed its concern about piracy on Mega sites and was replied to as set out below.

[257] Paragraph [128a]-[128d]:

The U.S. Attorney's Office for the Eastern District of Virginia expects a representative of the FBI to testify to the following facts:

---

<sup>72</sup> See SROC 1 paras [42]-[43] (ROC bundle pp 51-52).

a. According to a preliminary review of two e-mail accounts used by ORTMANN, abuse@megaupload.com and [mo@megaupload.com](mailto:mo@megaupload.com), between October of 2008 and October of 2011 ORTMANN and PayPal exchanged e-mails regarding copyright-infringing materials found on the Mega Sites.

b. During the 2010 calendar year, PayPal representatives sent ORTMANN over 115 notices referencing more than 2,000 URL links to copyright infringing materials on the Mega Sites. More than 94% of these URL links were uploaded by only 193 users with registered accounts on the Mega Sites (the remainder was uploaded by anonymous accounts). And the copyright infringing materials associated with these URL links were downloaded more than 700,000 times. During the 2011 calendar year, PayPal representatives sent ORTMANN over 30 notices referencing more than 1,400 URL links to copyright-infringing materials on the Mega Sites. More than 92% of these URL links were uploaded by only 140 registered users (the remainder was uploaded by anonymous accounts). And the copyright-infringing materials associated with these URL links were downloaded more than 99,000 times.

c. ORTMANN responded to these copyright-infringement notices by assuring PayPal that the infringing file had been removed or deleted, and — for approximately 220 of the approximately 330 registered users — that the user had been blocked from using the Mega Sites (for the remaining users, ORTMANN either failed to mention the user entirely, or he indicated that the user had been warned). For example, on or about September 17, 2011, ORTMANN wrote the following two-sentence response: “All infringing uploads have been deleted and their uploader blocked. Thank you for forwarding this DMCA notice!”

d. A preliminary review of the databases shows that despite ORTMANN’s claims that the uploaded files had been deleted, the Mega Conspiracy merely disabled the specific URL links identified in the notices. And despite ORTMANN’s claims that approximately 220 registered users had been blocked, as of January 19, 2012, only approximately 18 of those users were blocked from using the Mega Sites on that date.

*Inference:* Dishonest assurances were made to Paypal about the treatment of reported copyright infringement.

*The alleged deception of the United States Trade Representative by Mathias Ortmann*

[258] These alleged false representations are discussed in paragraph [164]:

The USTR is an agency of the United States government, separate from and independent of the US Department of Justice. In December 2011, it named Megaupload in a review of “Notorious Markets”. Among other things, this report listed markets, including Internet sites, reputedly engaged in piracy and which “may merit further investigation for possible intellectual property rights infringements”. Particular reference was made to Megaupload’s rewards scheme and its role in distributing protected content.

Mathias Ortmann wrote to the USTR protesting the inclusion of Megaupload. To distance Megaupload from other pirate sites identified in the report (including “ThePirateBay” website), Ortmann made a number of representations which were clearly false.

[259] Mr Ortmann minimised the nature and significance of the rewards programme by:

- (1) Claiming it had not been “targeted at inducing infringing behaviour”;  
and
- (2) Implying that it was unpopular and therefore unsuccessful.

Behind the scenes the rewards scheme was regarded as Mega’s “growth motor”. It was known the scheme attracted uploads of infringing content and the appeal of this material substantially drove traffic to the Mega sites. It was thought necessary to maintain the incentive to upload popular infringing content, preserve access to it, and deceive aggrieved copyright owners about its continuing availability. Rewards were knowingly paid to users for infringing content.

- (3) He claimed that infringing content was rapidly taken down upon notification, and that “[d]irect real-time takedown access” was granted to “trusted partners”.
- (4) He claimed that Mega enforced a repeat infringer policy, when in fact it had protected and encouraged the activities of flagrant repeat infringers.
- (5) He claimed that “Over 15 million user uploads” had been removed for infringement, when in fact no “uploads” (i.e. files or content) had been removed for infringement.
- (6) He claimed that 100% of “files that are reported to be infringing are removed from the website... within 24 hours.” Files were not deleted but only individual reported URL links. Similarly, he represented that the Abuse Tool conferred the ability to remove “files” directly from the system “rather than having to go through a formal takedown process.”

*Inferences:* In this correspondence, Mr Ortmann criticised competitors of Mega for the kind of conduct that his own business had engaged in. This implies an appreciation that its own conduct had involved “illegal business practices”.

[260] Mr Ortmann acknowledged that “U.S. law requires removal of infringing files from servers within the U.S., but Mega removes infringing files from all of its servers worldwide – not just in the U.S.” The practice of preserving notified infringing files was therefore unlawful and had to be concealed. He knew the operation of the rewards scheme had been unlawful and therefore its real nature had to be concealed.

[261] Because Mr Dotcom:

- (1) made all ‘major decisions’ about the business;
- (2) discussed with the conspirators (especially Mr Ortmann) other legal threats to the Mega business; and
- (3) corresponded with Paypal in a similar manner, highlighting the “criminal activity” of competitors while hiding Mega’s use of the impugned practices;
- (4) it is reasonable to infer that he was aware of Mr Ortmann’s overture to the United States Trade Representative (USTR) and shared his knowledge that Mega’s own unlawful practices would need to be disguised if their company were to be removed from the list.

### ***Auditing***

[262] The applicant alleges that Mega claimed to have a rigorous auditing system involving an abuse or audit team to deal promptly with complaints from copyright owners, including complaints about the rewards system.

[263] Mega also screened for child pornography. One of the main functions of the audit team seems to have been the removal of other pornographic material from Megaupload and Megavideo to Megaporn/Megarotic.

[264] Auditing procedures also involved some examination of the content uploaded to Mega sites, in particular the visible content on Megavideo. Mr Ortmann was therefore careful not to reveal anything that showed Mega was “not the dumb pipe we claim to be.” At paragraph [103rr] Mr Ortmann refers to infringing material on Megavideo, reminding Mr van der Kolk:

the important thing is that nobody must know that we have auditors letting his stuff through.” ... “if we had no auditors – full DMCA protection, but with tolerant auditors, that would go away.

[265] The auditing priorities are made clear in guidelines that Mr van der Kolk emailed to an employee in 2007. Paragraph [74b] sets out these guidelines:

Megarotic Video: Videos that have to be set to private:  
 - Long length high quality videos that are obvious ---  
 - Video with known logos / website URL's in it of copyright holders

Megavideo:  
 - Mark sexy / soft erotic (non nude) videos as private  
 Delete soft erotic with nudity  
 - Delete pornographic / extreme nudity (visible organs / penetration /etc.) and block the user  
 - Delete hateful / violent content (obvious racism / real killing /torture, etc.)

Auditing for Megavideo is rather simple, just make sure that the above described stuff will be deleted and the rest of the videos can be approved.

[266] Paragraph [74b] continues:

Videos that were set to "private" were not publicly displayed on the front pages of the Mega Sites, but users still had the ability to distribute these URL links in the same manner as non-private links, for example, on third party linking sites.

*Inference:* Auditing procedures allowed copyright infringing content to be hosted, but its presence was concealed by assigning it a ‘private’ (i.e. non-searchable) status on the Mega sites.

[267] The applicant's evidence highlights the procedures that Mega claimed to adopt to prevent the storage and transfer of child pornography. Paragraphs [31f]-[31f 1-2] set out these procedures:

E-mails between conspirators demonstrate that the Mega Conspiracy has eliminated known child pornography and other illicit content, including terrorist propaganda videos, by searching the system for identical MD5 hash values and deleting files with matching hash values. Members of the Mega Conspiracy have failed to implement a similar program to actually delete or terminate access to copyright-infringing content.

i. On or about April 8, 2007, DOTCOM sent an e-mail to PayPal, in which he stated that Megaupload.com was working toward "preventing pedophiliac materials from being distributed through our service[.]" DOTCOM outlined their "key procedures", which included the following:

1. Keyword-based upload alerting. We maintain a list of patterns/words commonly used in relevant file names and descriptions. Whenever a new file is uploaded whose file name or description matches, the file is forwarded to our content auditing team for further inspection.

2. Recursive tracking of uploaders and files. When our team of content auditors receives a notification of an upload related to child exploitation either through (1), or from a 3rd party source, they verify the file's nature, then cross-match related uploads by IP, by the file's hash fingerprint, and by the supplied uploader credentials (user ID, e-mail addresses). This procedure is effective, because the same uploader often uploads more than one file, and the same file is typically uploaded more than once by different, unrelated persons. The process is applied repeatedly, leading to a step-by-step compromise of most file portfolios containing pedophiliac material. Existing fingerprints are stored permanently and will immediately trigger an alarm if they match a new upload. The Mega Conspiracy failed to implement any similar procedures for copyright-infringing works.

[268] Mr Dotcom's reassurance about Mega's auditing ability is again shown at paragraph [31f iii]:

On or about August 14, 2010, DOTCOM sent an e-mail to hosting company executives DS and JK, and to Ortmann. In the e-mail, DOTCOM addressed the Mega Conspiracy's treatment of "Content that is illegal per se, most notably pedophilia material." DOTCOM stated, "A specialized team of auditors is continuously putting great efforts into the discovery and elimination this type of content by looking at upload sources (user accounts, IP addresses) of newly reported files, then identifying similar items uploaded from the same source, leading to further upload sources. This process is applied recursively and exhaustively[.]" DOTCOM further stated, "As a result, the frequency of notices coming from established monitoring bodies such as 'Telefono Arcobaleno' has decreased to near-zero as it is now well known in the criminal scene that abusing Megaupload for storing their appalling material would pose great risks to them."



*Inference:* The respondents did not use the auditing capabilities they possessed to disable access to identified copyright infringing files.

[269] The applicant alleges the inferences are confirmed by the evidence of Andrus Nomm. Mr van der Kolk’s auditing team in the Philippines “was not very effective and... many of the auditors did not even know what copyright was.” Its work was “not a serious effort and was more about appearances than effectively addressing infringement”.<sup>73</sup>

*Inference:* It was convenient for Mega to be able to say that it had a dedicated, efficient team who filtered uploads for copyright infringement but, in reality, this was just another part of the façade of complying with copyright obligations.

[270] Mr Nomm provides other examples of how techniques that could have been used to curb infringement were deliberately eschewed. In 2009, he proposed an “automatic system for finding copyright-infringing files on Megavideo.com and flag them for review by an auditor.” It involved checking video files “for watermarks and other indicators that were suggestive of copyrighted material.” Mr Ortmann rejected the idea because “it would prove that they had the ability to easily filter content on Megavideo.com”<sup>74</sup>.

[271] The applicant alleges that Mr Ortmann used a “video-querying tool” tool to identify high definition videos that could be exploited on Megavideo. These clips were unlikely to be user-generated content, borne out by the hundreds of videos sent on to Mr Nomm for review. He found that “many of the videos were copyrighted motion pictures and television shows.” A technique that could have been used to curb infringement was therefore used for the opposite purpose.<sup>75</sup>

### **Non-searchability and the sanitising of front pages**

[272] The applicant alleges that the content of Mega could not be directly searched within the site, and although Mega has portrayed this as a privacy and

---

<sup>73</sup> SROC 6 para [170u] (ROC bundle p 312).

<sup>74</sup> SROC 6 para [170v] (ROC bundle p 312).

<sup>75</sup> ROC para [17] (ROC bundle pp 5-6).

anti-infringement feature, its encouragement of infringement through external “linking” sites makes this a hollow claim.

[273] Mega did provide a “Top 100” page. This purported to list the most popular downloads on Mega, but it was deliberately sanitised to conceal the popularity of infringing files.<sup>76</sup>

[274] In 2008, Mr Ortmann expressed his hope that the “Top 100” might itself bring in significant revenue. Mr van der Kolk’s response in paragraph [103bb]<sup>77</sup> referred to its primary function – to make the site look “legit”:

“yeah, and it makes our whole site look much more legit & attractive as well,”  
to which ORTMANN replied, “exactly.”

[275] A message from Mr van der Kolk in 2009 illustrates how the “Top 100” was manipulated. At paragraph [30]:

On or about October 25, 2009, Mr van der Kolk instructed a Mega Conspiracy employee through an e-mail, written in Dutch, how to alter the “featured” videos list on Megavideo.com and the “Top 100” list on Megaupload.com. Mr van der Kolk wrote, among other things, that the Top 100 should not list any copyrighted files, but instead should list game demos, software demos, and movie trailers. Mr van der Kolk instructed the employee to track what was currently popular on the Internet and to download material from websites such as download.com, apple.com/trailers, and gamespot.com. Mr van der Kolk further instructed the employee to create fake accounts on Megaupload.com and Megavideo.com and to upload the files to those accounts, so that it would appear that the files were uploaded by active users instead of Mega Conspiracy employees.

*Inference:* The front pages of Mega were manipulated to conceal the popularity of infringing content and convey the false impression that the most popular content did not infringe copyright. Andrus Nomm confirms the validity of this inference.<sup>78</sup>

[276] Paragraph [40b] shows how Agent Poston found some infringing content, but by browsing rather than using the search function.

In an undercover capacity, Agent Poston browsed the front page of Megavideo.com, which does not show any obviously infringing copies of any

---

<sup>76</sup> SROC 6 para [170U] (ROC bundle p 312).

<sup>77</sup> (ROC bundle p 139).

<sup>78</sup> SROC 6 para [170gg] (ROC bundle p 314).

copyrighted works. Instead, the page contains videos of news stories, user-generated videos, and general Internet videos in a manner substantially similar to Youtube.com. Agent Poston's analysis further showed that the Megavideo.com website allowed users to search for video files and to browse video files under categories such as "Entertainment," "Comedy," "Music," and "Video Games." While browsing under the "Entertainment" category, Agent Poston successfully viewed a number of copyright infringing video files, including motion pictures. Conducting a search for the files' titles through the Megavideo.com search function, however, did not reveal the existence of these copyright-infringing titles in the returned search results.

[277] Paragraph [102c] explains that further steps were taken to keep infringing content off the front page.

Software written by ORTMANN and VAN DER KOLK marked all videos longer than 10 minutes as private. This ensured they were not publicly displayed on the front pages of the Megavideo website.

*Inference:* On Megavideo, the availability of copyright infringing files was deliberately concealed.

[278] The applicant alleges that it was clear that the public content of Megavideo was not the basis of its profitability. Paragraph [103tt] shows this in plain language:

On or about November 21, 2009, via Skype, ORTMANN told VAN DER KOLK, "MV's public videos could not possibly have generated significant payments."

*Inference:* On Megavideo, the availability of copyright infringing files was deliberately concealed.

[279] The applicant alleges that it was a perennial problem for Mega to maintain the sanitised appearance of Megavideo, while creating the appearance of a flourishing site specialising in non-copyright video. In an early conversation on this issue, Mr Ortmann referred to the legal risks of exposing the availability of infringing video material.

[280] Paragraph [103s]:

On or about November 22, 2007, via Skype, VAN DER KOLK said to ORTMANN, "damn the top favorites on MV really need some cleaning indeed" and ORTMANN responded, "we seem to have two main types of content on MV: softcore nudity and simpsons :)" ORTMANN also said, "if Fox TV sends us a takedown request, our Gmail accounts will overflow," and

“if someone starts exploring our sites and experimenting a bit, we’ll be down in no time.” The Simpsons is a copyrighted television program

*Inference:* It was thought necessary to conceal the popularity of copyright content available on Megavideo.

[281] In 2009, Mr van der Kolk and Mr Ortmann spoke about the sanitising of Megavideo in this manner:<sup>79</sup>

“Theoratically we could make MV just like MU,” “remove all the video listing stuff.” ORTMANN responded, “yep, but even better than that, we list only really harmless stuff,” and VAN DER KOLK replied, “yes, but problem is almost no harmless stuff is being uploaded to MV :)” Then VAN DER KOLK suggested, “We should actively add youtube videos again perhaps,” and ORTMANN responded, “yes, we could do that indeed.” ORTMANN suggested, “Kim’s idea of leaving the semi-harmful stuff online for 23 hours is also pretty good,” and VAN DER KOLK responded, “yes also not bad,”....

*Inference:* It was known that most of the content uploaded to Megavideo was subject to copyright, a fact that needed to be concealed.

[282] Paragraph [148c] shows how, in 2011, Mr Dotcom was dissatisfied with the stale appearance of Megavideo’s front page. Viewers could see that the show-cased files had been uploaded several days ago. He instructed Mr van der Kolk to mix older content with recent uploads, to create the illusion of flourishing upload activity based on non-infringing content.

As referenced in Paragraphs 18 and 30 of the Record of Case, the defendants made Megavideo's front page appear more legitimate by screening out copyright-infringing content, in particular from the Top 100 list. After such content was eliminated, however, there was apparently so little remaining content that on or about December 21, 2011, via Skype, DOTCOM told VAN DER KOLK, "I need someone to implement the reupload logic we discussed some time ago. it is not good what’s happening now with videos on the first page listed as uploaded 2 days ago." VAN DER KOLK responded, "Okay, I will try to come up with something for that asap." DOTCOM then instructed VAN DER KOLK, "just reupload everything from 2 years ago in the same order. same user names, everything[,] and mingle with the new uploads." VAN DER KOLK responded, "Yes sir, will do that."

*Inference:* The need to disguise the hosting of infringing content led to creative manipulation of Megavideo’s front pages.

---

<sup>79</sup> Para [143rr] (ROC bundle pp 142-143).

[283] The applicant alleges that the auditing process mentioned at paragraph [284ff] above should have curbed the appearance of infringing content on the public pages of Megavideo. Mr Dotcom was highly sensitive about the detection of infringing content in such places. Paragraph [103ss] shows how in late 2009, he thought the auditing process had failed and admonished Mr van der Kolk for letting “the latest commercial stuff” appear on public pages:

On or about November 19, 2009, via Skype, DOTCOM sent ORTMANN a Skype conversation between DOTCOM and VAN DER KOLK, during which DOTCOM said: MV is full of problematic content on the [publicly viewable] video pages. I told you how important this is. Every day counts, especially since we have articles out there comparing us with napster and putting us in a bad light. WHY THE FUCK did you not take care of this? You told me you will do this WHILE you are in HK. I just spoke with mathias [ORTMANN] and he told me he informed you long time ago about fixing this. WHY do you risk our good running business with not following up on important matters like this. If you look at the latest video pages now it is FULL with the latest commercial stuff. FUCK THIS BRAM! VAN DER KOLK responded, “I already spoke to Mathias, and will implement some new measures now. I also have a meeting with the auditors tomorrow evening, I always pointed out to them how important it was that all big hollywood stuff needs to go, but apperantly they’re not doing a good job.” DOTCOM replied: ITS your job, when a task like this is given to you, that you make sure it is properly done. This is YOUR fault and not the auditors. And Mathias brought this to your attention months ago when I told Mathias about it and asked this to be fixed with filters, etc. You are responsible Bram if this backfires because it hasnt been done. Better make sure that by Monday I will never see shit like this again on the public video pages or else we will have a major problem again, understood?

*Inference:* Auditing procedures allowed infringing content to be hosted, but were intended to disguise the availability of such material.

[284] The applicant alleges that the general non-searchability of Mega sites – the “innocent front end” – was a critical factor in deflecting the scrutiny of copyright owners, while piracy flourished through the “private backend”, via links published on the internet. Non-searchability was a point of distinction with certain other sites, which ran the risk of exposing the content they hosted. This is the distinction referred to by Mr Ortmann in a message from 2011. Mega was safer because infringing content could not be located by direct searching. Paragraph [38w] describes this:

On or about October 10, 2011, JK, an executive from a hosting provider, sent an e-mail to Ortmann entitled "Article." The e-mail contained a link to a news

article, which discussed how a Dutch court ordered a "major" website "to delete all infringing content from its servers." The article asked: "Could file-hosting services like MegaUpload and RapidShare be next?" In the e-mail, JK asked Ortmann: "Do you have any concerns that this kind of thing could find its way to you"? Ortmann responded to JK, with a copy to DOTCOM, stating that the sites in the article "provide a search index covering their entire content base, including the infringing material." As described above, Megaupload.com did not provide any search index whatsoever to the public, but had an internal index that reveals many hundreds of thousands of copyright-infringing works on the Mega Sites.

*Inferences:* The infringing content hosted on Mega could easily be identified by the respondents. At the same time the absence of any public search function made it harder for copyright owners to detect infringement.

[285] The applicant says Mr Batato made similar observations in discussing the takedown of Kino.to. Mr Batato thought that the Kino.to site hosted files and paid users to upload content. In this respect it resembled Mega. The third aspect of its operation involved running a referrer site, which would associate Kino.to with the content it hosted. Mr Batato thought the combination of these three elements was "crazy". (This conversation occurred in June 2011, the same month in which Mega ended its rewards scheme. In the wake of the Kino.to takedown, Mr Dotcom thought that Ortmann should not be flying to Germany).<sup>80</sup>

[286] In August, Mr Batato also discussed Kino.to with Mr Ortmann, calling it "super fraud" and "organised crime". Mr Ortmann agreed that "we have to separate ourselves from that." Paragraph [155c] reproduces this discussion:

As referenced in Paragraph 39(p) of the Record of Case, Kino.to was a third-party linking site that regularly linked content to the Mega Sites. On or about June 13, 2011, via Skype, BATATO and a third-party discussed Kino.to being closed down by European law enforcement. BATATO wrote, "That was expected . . . They were crazy to run a hoster AND a referrer site AND pay people to upload stuff." On or about August 8, 2011, via Skype, BATATO said to ORTMANN in German that what Kino.to did "was really super fraud. You can practically call it organized crime." ORTMANN responded, "Exactly. And we have to separate ourselves from that." BATATO agreed, "yes." In this context, it appears that BATATO and ORTMANN were expressing confirmation of their decision to prevent users from searching the Mega Sites for copyright-infringing materials and to rely on third-party linking sites to index and link to infringing content.

---

<sup>80</sup> See ROC para [38u] (ROC bundle p 38).

*Inference:* The respondents appreciated that providing an indexing or referrer service to the content they hosted would expose the extent of their criminal copyright infringement. The absence of a public search function was viewed as a protective measure.

### ***Mass Copying of YouTube Videos***

#### *Information*

[287] The applicant alleges that in 2006-2007, the respondents directly infringed en masse video clips from YouTube and used them to “populate” Megavideo.com. The objective was to convey the false impression that this site “hosted primarily user generated content instead of copyright-infringing content”.<sup>81</sup> Mr Dotcom, for instance, claimed in 2009: “The vast majority of users is uploading home videos, web cam captures, content they own or have the right to copy and other legitimate content”.<sup>82</sup> This was a claim that the acquisition of YouTube videos enabled him to make, with some semblance of plausibility. YouTube videos were used for this purpose at least until 2011.<sup>83</sup>

#### *Breach of copyright*

[288] The applicant alleges that this act was itself a major breach of copyright. Paragraphs [26b]-[26c] explain the US expects to lead evidence at trial that:

According to the YouTube "Terms of Service," users who upload content to YouTube retain all of their ownership rights in their content. By uploading their content to YouTube, however, such users grant YouTube a license to use, reproduce, and distribute such content.

In general, the further reproduction and distribution of videos that are taken from the Youtube.com platform violates the copyright of the individual who uploaded that video to Youtube.com.

Paragraph [27] explains that the applicant also expects:

...users who uploaded content to Youtube.com, and who retained copyright ownership in such uploaded content, to testify that the infringing copies of their copyrighted works were reproduced and distributed for commercial

---

<sup>81</sup> Superseding Indictment, para [63].

<sup>82</sup> ROC [38m] (ROC bundle pp 36).

<sup>83</sup> ROC para [28h] (ROC bundle p 20).

advantage and private financial gain by the Mega Conspiracy on the Mega Sites without authorization.

[289] The applicant says that the programme used to transfer the YouTube content imported each file into the account of a randomly-selected user of the Mega sites. The video was also assigned a false “view” count. The operation of the programme in this manner is confirmed by the analysis of a computer specialist and the observations of those who found their YouTube material on Megavideo. In furtherance of the deception, copyright owners who complained about the presence of their material on Megavideo were told, falsely, that the accounts of the supposed Megavideo users had been terminated.<sup>84</sup>

*Inference:* The YouTube copying exercise was a fraud on the owners of copyright in the clips, which was directly committed by the respondents. Video material was acquired from other tube sites for the same purpose.

*Dialogue about the YouTube copying*

[290] The applicant alleges that the unfolding of the project is reflected in a series of emails and Skype exchanges set out below in chronological order. The inferences they say may be drawn from this correspondence include the following:

- (1) The respondents understood they were engaged in fraudulent conduct. They expected their leeching software to be blocked at some stage, and to encounter legal difficulties as a result of what they were doing.
- (2) YouTube videos were fed through the Megavideo site in way that made the site appear to be growing very rapidly on the basis of “user generated content.”
- (3) It was anticipated that displaying the YouTube content would combat Megavideo.com’s “piracy reputation.”
- (4) By making the site appear legitimate, it was hoped that potential buyers or investors would be deceived about the real basis of the site’s popularity.

---

<sup>84</sup> ROC para [28e]-[28g] (ROC bundle p 20).



[291] The extracts of the respondents' discussion of the YouTube project between 10 April 2006 and 10 October 2009 are:

10 April 2006, at paragraph [28b]:

On or about April 10, 2006, Van der Kolk sent an e-mail to Ortmann asking, "Do we have a server available to continue downloading of the Youtube's vids? ... Kim just mentioned again that this has really priority." In addition, Van der Kolk wrote, "Hope [Youtube.com] is not implementing a fraud detection system now... \* praying \*". Van der Kolk also wrote: "Well we only have 30% of their videos yet.. In my opinion it's nice to have everything so we can descide and brainstorm later how we're going to benefit from it."

11 February 2007, at paragraph [28c]:

On or about February 11, 2007, Van der Kolk sent an e-mail to Ortmann indicating that "Kim really wants to copy Youtube one to one."

17 May 2007, at paragraph [105b]:

On or about May 17, 2007, via Skype, VAN DER KOLK said to ORTMANN, "he [DOTCOM] was telling again yesterday how important 'all youtube files' are and that I need to ask you for more disk space so we can leech." VAN DER KOLK also said, "I'll just stick to our strategy and leech most popular files only." ORTMANN responded, "right, very good."

4 June 2007, at paragraph [105c]:

ORTMANN, "Andrus [NOMM] told me everything is done to import the Youtube video's?" ORTMANN responded, "Andrus [NOMM] has finished the flv indexer... his approach is pretty ingenious, we'll be able to import everything within a few days." VAN DER KOLK responded, "Cool! :-)". The acronym "flv" refers to the Flash Video file type.

14 June 2007, at paragraph [105d]:

On or about June 14, 2007, via Skype, VAN DER KOLK said to ORTMANN, "Youtube will be pissed :-)". ORTMANN responded, "heh :) indeed... I think we'll just do the importing by direct fetching from one of our servers initially until they block us."

19 June 2007 at paragraph [105e]:

On or about June 19, 2007, via Skype, VAN DER KOLK said to ORTMANN, "to have the top XXX thousand videos for the launch of MV is nice", "but having ALL youtube files is over the edge." VAN DER KOLK then said, "but it was always very hard to say anything about it." The acronym "MV" refers to Megavideo.com. ORTMANN responded, "yeah, it's Kim's pet project :)" And VAN DER KOLK replied, "kim was extremely persistant".

27 June 2007 at paragraph [105f]:

On or about June 27, 2007, via Skype, VAN DER KOLK asked ORTMANN, “Do you think it will be possible to start importing the youtube video to Megavideo today or tomorrow?” ORTMANN responded, “today, definitely. No more delays.” VAN DER KOLK replied, “okay that sounds good :-)” and, “If there’s anything I can help you with, please let me know!”

5 August 2007 at paragraph [105g]

On or about August 5, 2007, via Skype, VAN DER KOLK said to ORTMANN, “Hopefully youtube will not block us and will not do anything evil,” “but if we get letters from their lawyers and we let [unindicted conspirator] read then we’ll definitely get big instantly haha.” ORTMANN responded, “I am sure we’ll get a letter from their lawyers sooner or later and that our leech IP will be blocked.”

3 September 2007, at paragraph [105h]:

On or about September 3, 2007, via Skype, VAN DER KOLK and ORTMANN discussed copying, without authorization, videos from websites such as YouTube.com, Break.com, and Google Videos. ORTMANN stated, “I have 152589 successful imports in the db, this seems quite a lot.” The acronym “db” refers to database.

4 October 2007, at paragraph [105i]:

On or about October 4, 2007, via Skype, VAN DER KOLK sent to ORTMANN a conversation between VAN DER KOLK and DOTCOM, where DOTCOM stated, “the day has 1440 minutes and I want to see one Video upload on megavideo every minute. If necessary use the youtube videos we still have unpublished and publish one by one from dirrent accounts every minute,” and “otherwise we look like small fish shit.” VAN DER KOLK commented to ORTMANN, “I was thinking to automatically import 1000 youtube videos every day to fulfill Kim’s wish (and it would make MV look better).” ORTMANN responded, “good idea indeed!”

8 October 2007, at paragraph [105j]:

On or about October 8, 2007, via Skype, ORTMANN asked VAN DER KOLK, “so, how can we have a new youtube import online every minute without 24h auditor surveillance?” VAN DER KOLK responded, “youtube videos are already audited, some videos that were imported by users were ‘sexy’ but there’s never real nudity on youtube.” ORTMANN replied, “okay, so we trust them...” VAN DER KOLK then said, “so far youtube imports didn’t require approval as well” “and, I only import popular videos from youtube every minute.” ORTMANN responded, “but there should be a youtube import completing every minute anyway... the importer is working heavily all the time.”

9 October 2007, at paragraph [105k]:

On or about October 9, 2007, via Skype, ORTMANN asked VAN DER KOLK, “is youtube importing still working, btw?” VAN DER KOLK responded, “yes it’s working perfect now!” and “the recent videos on Megavideo look so much better.” He also said, “and I’m automatically leeching the featured break videos to feature on Megavideo, so Megavideo looks much more alive now.” ORTMANN responded, “perfect,” “(and nasty :).” The phrase “break videos” appears to refer to videos copied from the website Break.com. VAN DER KOLK then said, “Now Kim can try to get some advertisers or investors or buyers for it :-)” “and semi scam then :-)” ORTMANN responded, “yeah :)”

14 April 2008, at paragraph [105l]:

On or about April 14, 2008, via Skype, VAN DER KOLK asked ORTMANN, “What was the proxy server again that was setup for youtube importing about two months ago?” ORTMANN responded with the server’s Internet Protocol address, and roughly thirty minutes later VAN DER KOLK said, “now let’s activate the one video per minute script again so that MV looks nice again.” ORTMANN commented, “yeah, that would be cool.”

18 April 2008, at paragraph [105m]:

On or about April 18, 2008, via Skype, ORTMANN told DOTCOM, in German, “let’s see, if TF1 will sue us for 10s of millions aside from Dailymotion and Youtube :)” TF1 is a private national French television channel. The website Dailymotion.com is a French videosharing website, similar to YouTube, on which users can upload, share, and view videos. In addition to YouTube, the Mega Conspiracy copied without authorization videos from Dailymotion.com.

18 April 2009, at paragraph [105n]:

On or about April 18, 2009, via Skype, ORTMANN and VAN DER KOLK discussed videos appearing in Google searches. VAN DER KOLK said, “maybe we should slowly do that again, it really makes the site look more legit,” and ORTMANN responded, “yes.” VAN DER KOLK asked, “How did we do it last time, I downloaded the files directly to a fileserver right?” and ORTMANN answered, “yes.” VAN DER KOLK then said, “I’ll try to quickly implement something with the Youtube API so that we can upload new legit videos to MV continuously to make the site look more legit.” VAN DER KOLK commented, “Megavideo has quite a piracy image already,” and ORTMANN added, “yes.”

10 October 2009, at paragraph [103rr]:

On or about October 10, 2009, via Skype, VAN DER KOLK told ORTMANN, “Theoratically we could make MV just like MU,” “remove all the video listing stuff.” ORTMANN responded, “yep, but even better than that, we list only really harmless stuff,” and VAN DER KOLK replied, “yes, but problem is almost no harmless stuff is being uploaded to MV :)” Then VAN DER KOLK suggested, “We should actively add youtube videos again perhaps,” and ORTMANN responded, “yes, we could do that indeed...”

## **Prima Facie Evidence that the Individual Respondents were Members of the Conspiracy to Defraud Copyright Owners**

### **Introduction**

[292] The applicant alleges that there is evidence establishing that each of the respondents was a member of the conspiracy alleged in the counts.

[293] The application says that participation in the conspiracy is demonstrated by inferences drawn from a broad range of statements and circumstances.

[294] They say the evidence needs to be assessed against the background of a closely held business, controlled by a few people who were well known to each other.<sup>85</sup>

### ***Evidence that Kim Dotcom was a member of the copyright conspiracy***

[295] The extracts of the respondents' discussion of the YouTube project between 10 April 2006 and 10 October 2009 are:

#### ***Ownership and financial interests***

[296] In paragraph [22d]:

In a sworn declaration, dated December 14, 2011, DOTCOM declared as follows: "I am the Chief Innovation Officer of Plaintiff Megaupload Ltd. ('Megaupload'), and have been employed at Megaupload since September 2005." E-mails sent between conspirators demonstrate that prior to becoming the Chief Innovation Officer, DOTCOM was the Chief Executive Officer for Megaupload Limited between September 2005 and August 2011. E-mails between conspirators further show that DOTCOM is the head of the Mega Conspiracy, which employs more than 30 people residing in approximately nine countries; he has supervised the development of the websites and companies utilized in the Mega Conspiracy; he has directed the creation of the network infrastructure behind the Mega Sites; he has negotiated contracts with Internet Service Providers and advertisers; he has administered the domain names used by the Mega Conspiracy; and he exercises ultimate control over all major decisions in the Mega Conspiracy. E-mails show that DOTCOM has arranged millions of dollars in payments for the computer servers utilized by the Mega Sites around the world, and has also distributed proceeds of the Mega Conspiracy to his co-conspirators. As described below, DOTCOM owns approximately 68% of Megaupload.com and all of Megavideo.com. Additionally, as described below in the section entitled DOTCOM's Knowledge of Copyright Infringement, e-mails show that on numerous

---

<sup>85</sup> See SROC 2 para [136a] (ROC bundle p 229).

instances, DOTCOM received DMCA copyright infringement takedown notices from third-party companies, and further, that DOTCOM has personally received at least one infringing copy of a copyrighted work on a Mega Site. According to an internal financial statement for Megaupload Limited, DOTCOM received more than USD \$42 million from the Mega Conspiracy in calendar year 2010 alone.

[297] Mr Dotcom opened a PayPal account for Megaupload Limited in 2005 and a DBS Bank account for the same company in 2006.<sup>86</sup> His control over the finances of the Mega businesses is explained in paragraph [41d]:

E-mails sent between conspirators demonstrate that DOTCOM had the authority to distribute funds from the Mega Conspiracy's main financial accounts. For example, on or about June .15, 2010, and again on or about June 1, 2011, and on or about November 11, 2011, the Chief Financial Officer ("CFO") of Megaupload Limited sent e-mails to DOTCOM, asking: "Please authorize the following payments[.]" In the June 15, 2010 e-mail, the payments included the following: USD \$30,292 for the purchase of new Internet domain names; and HKD \$12,816.32 for an American Express business credit card. In the June 1, 2011 e-mail, the payments included the following: USD \$93,621.60 to Cogent for the payment of Internet bandwidth, hosting, and support services relating to the Mega Sites; and USD \$951,112 to Carpathia for the payment of hosting and support services relating to the Mega Sites. The CFO noted that the Carpathia invoice had been "approved by Mathias [Ortmann]". In the November 11, 2011 e-mail, the payments included USD \$125,000 for the services of a digital advertising agency.

*Inference:* Dotcom occupied such a controlling position in the affairs of the business that it is reasonable to infer he knew of and participated in the conspiracy to defraud copyright owners.

### **Dotcom personally oversaw development of the websites and associated companies**

[298] Paragraph [136k]:

On or about September 7, 2005, DOTCOM registered the company Megaupload Limited in Hong Kong, as described in Paragraph 22(f) of the Record of the Case.

[299] Paragraph [136m]:

On or about May 20, 2006, DOTCOM registered the companies Megamedia Limited and Megavideo Limited in Hong Kong, as described in Paragraphs

---

<sup>86</sup> See ROC para [41a]-[41b] (ROC bundle p 45).

22(o) & (p) of the Record of the Case. Also on May 20, 2006, DOTCOM registered the company Megarotic Limited.

*Dotcom personally negotiated the Cogent Communications and other server network contracts*

[300] Paragraph [72b]:

DOTCOM personally negotiated the terms of the contractual agreement with Cogent Communications ("Cogent"), the Internet hosting provider that owned the computer servers located in Washington, D.C. Between at least October of 2008 and January of 2012, the Mega Conspiracy leased bandwidth and, beginning in December of 2010, these servers, maintaining exclusive possession and access, except for maintenance and support work performed by Cogent. DOTCOM also personally negotiated the terms of the contractual agreements with Carpathia Hosting, Inc. ("Carpathia"), and Leaseweb. Between at least September of 2005 and January of 2012, the Mega Conspiracy leased servers from Carpathia, maintaining exclusive possession and access, except for maintenance and support work performed by Carpathia. Between at least April of 2007 and January of 2012, the Mega Conspiracy leased and also purchased servers from Leaseweb, maintaining exclusive possession and access, except for maintenance and support work performed by Leaseweb.

[301] Paragraph [38g]:

On or about August 11, 2008, DOTCOM requested that the Mega Conspiracy's contract with Leaseweb drop a standard clause requiring contract termination for violations of Leaseweb's "Acceptable Use Policy." The standard clause included, but was not limited to, violations regarding copyright infringement.

*Inferences:* Mr Dotcom was directly involved in the negotiation of key infrastructure contracts. The Cogent arrangement was a response to mass demand for highly popular copyright infringing works. It can be inferred that he knew the Mega business prospered from exploiting traffic to such material, and he took steps to enhance that traffic. He therefore allied himself with the conspiracy.

*Dotcom's role in the rewards scheme and payment of money to conspicuous repeat infringers*

[302] The applicant's evidence shows frequent discussions between Mr Ortmann and Mr van der Kolk about the operation of the rewards scheme. Mr Dotcom was also involved in Skype exchanges on this subject. He paid close interest in the activities of prolific uploaders and the growth in traffic that could be attributed to their content:

Paragraph [106i]:

On or about January 18, 2008, via Skype, DOTCOM asked ORTMANN, in German, "and I need to know exactly how much we pay monthly to uploader rewards." ORTMANN responded, "the first rewards payment after Christmas was 76K." DOTCOM replied, "maaaaddnnneess!" and then he said, "no wonder we're growing like that now." In addition, DOTCOM said, "have growth" "not because of gigs" but "because of PAYMENT!" ORTMANN commented, "the payment came after the growth :)" and DOTCOM responded, "since the special people uploaded and promoted more." ORTMANN agreed, "yes, that is surely relevant." DOTCOM then said, "growth has less to do with the many gigs than with the rewards. in my opinion." The term "gigs" refers to Gigabytes, a unit of measuring data-storage and file-size capacity.

[303] Paragraph [106k]:

[304] On or about January 26, 2008, via Skype, VAN DER KOLK sent ORTMANN a conversation between VAN DER KOLK and DOTCOM. During that conversation, VAN DER KOLK sent DOTCOM the rewards payments for a 2.5-week period. DOTCOM responded, "cool! "let's fucking pay." VAN DER KOLK replied, "okay I be less restrictive, fine with me :)" and DOTCOM responded, "good." DOTCOM also said, "this is our growth motor," "you will see."

[305] Paragraph [106l]:

[306] On or about February 17, 2008, via Skype, DOTCOM asked ORTMANN, in German, "do we know from the reward stats now who really brings us the sales?" ORTMANN responded, "bram is supposed to build a stats tool for that... then we will have a slider too."

*Inferences:* Mr Dotcom knew of the rewards scheme and directed its administration. He appreciated that Mega's growth was directly related to users who uploaded infringing files and 'promoted' the availability of this content on third party sites.

*Repeat infringer TH*

[307] Paragraph [62e]:

On or about December 20, 2006, TH sent an e-mail to support@megaupload.com entitled "The Last Note." TH complained that he had not received a \$1,000 reward payment based on having accumulated 1,000,000 reward points in his premium account. TH stated that if he was not paid "within 24 hours," then he would expose the payment failure on "over 100 Vietnamese websites in the world." He further stated, "I really do not care about your payment or not. I do not give you a chance to cheat millions of user and uploaders anymore." On or about December 21, 2006, DOTCOM responded to ORTMANN and VAN DER KOLK, omitting TH, writing, "This

is the fifth e-mail from this guy. WHY THE [expletive redacted] DOES NOONE care. Bram was about to give me the final confirmation that the payment is legit, and I am sending it now."

[308] Paragraph [62u]:

On or about March 2, 2008, TH sent an e-mail to support@megaupload.com entitled "Reward points." TH wrote, "Please adjust the system for reward points as soon as possible. Because Available Points do not increase to match with Total Downloads that increase every hours. This problem lasts for 2 weeks. Please make a fair thing for uploaders." The following day, DOTCOM responded to ORTMANN, omitting TH, writing in German that it should give them pause when their main uploader complains. ORTMANN replied to DOTCOM that same day, writing in German that a new Uploader Reward policy was causing TH to lose points, and that TH will need to try harder if he wants to continue earning as much as \$10,000 per month through the program.

[309] Mr Dotcom also personally responded to TH's emails.

[310] Paragraph [62w]:

On or about March 19, 2008, TH sent an e-mail to supoortmegaupload.com entitled "Reward Points." TH complained about a new Uploader Reward policy that was causing TH to lose points. TH stated that if the policy was not adjusted, then he would "post on over 120 websites and notify users to stop buying premium account[s] with Megaupload." On or about March 19, 2008, DOTCOM responded to TH, writing, "You and your friends are at most 1% of our traffic. So please don't overestimate your importance to us. We are thankful for your support of Megaupload in the past and I think we have always been fair to you." DOTCOM further wrote, "In the future you will also earn rewards for every premium customer that you bring to us."

[311] Paragraph [62x]:

On or about May 10, 2008, TH sent an e-mail to support@megaupload.com. TH wrote, "I just came back to USA, and now my 11) for downloading or uploading from USA. I would like to start working for you now. Would you please let me know when the renovation will be done and how the new rule is? Thanks[.]" On or about May 11, 2008, ORTMANN responded, "Welcome back! The renovation is still in progress, but we can offer you a manual adjustment of your earned points according to the new standard as a special exception. Please send us a request before every redemption you plan to make." On or about May 12, 2008, DOTCOM responded to ORTMANN, omitting TH, writing: "Juhu. [TH] is back :-)" The German word "juhu" means "yay" in English.

[312] Paragraph [108c]:



On or about March 11, 2007, via Skype, DOTCOM asked ORTMANN, in German, “dude, can you give me the stats in connection of which user accounts have the most premium sales?” DOTCOM clarified, “I mean rewards users.” DOTCOM then said, “which uploaders have caused the most premium sales with their files.” Then DOTCOM stated, “I would like to know how much premium our [TH] has brought!”

[313] Paragraph [108d]:

On or about March 15, 2007, via Skype, DOTCOM asked ORTMANN, in German, “can you tell me how many premium accounts dear [TH] brought us? ORTMANN responded, “the analysis will take approximately 2 hours, I’ll work on that right away.” The following day, via Skype, ORTMANN said to DOTCOM, “morning...so far [TH] has provided us: -18 Million Download-Pageviews -112257 USD Premium-Sales to users who have downloaded at least 15 of his files.” DOTCOM responded, “112257????” ORTMANN then said, “yep, those are the global nguyens.” “Nguyen” is a common Vietnamese surname.

[314] Paragraph 108i]:

On or about March 20, 2008, via Skype, VAN DER KOLK sent ORTMANN a Skype conversation between VAN DER KOLK and DOTCOM, in which DOTCOM said, “i just sent a mail to [TH]. Check if he will make any major changes to his accounts or if his stats are dropping significantly in the next few days.”

*Inferences:* Mr Dotcom oversaw the administration of the rewards scheme. He closely followed the activities of a repeat infringer who received repeated payments under the rewards programme. He appreciated that this user was responsible for bringing significant traffic, which was attracted by the repeat infringers uploaded content. He therefore knew of, and aligned himself with, the conspiracy to defraud copyright owners.

[315] Paragraph [123a]:

On or about January 25, 2008, via Skype, ORTMANN told VAN DER KOLK, “user [AT] has sold 782 premium accounts since Dec 09,” commenting “not even a Vietnamese.” VAN DER KOLK responded, “wow!” ORTMANN then said, “he has 2 million reward points, used 1.3million.” ORTMANN then listed the top four registered users who caused other users to purchase premium accounts. A few minutes later, ORTMANN told DOTCOM, in German, “[AT] in 1st place with 782 Sales.” During the same conversation, DOTCOM pointed out that the 3<sup>rd</sup> place user “has 2.3 million reward points and 4,000 files” and then asked, “did we not pay him?” ORTMANN responded, “he is #3 in top sales.” DOTCOM stated that “he wants his money” and directed ORTMANN, “by all means pay [him].”

*Inference:* Mr Dotcom monitored the administration of rewards payments and appreciated the relationship between copyright infringement and business growth.

[316] Paragraph [110uu]:

The Mega databases indicate that TE's account was deactivated in 2008 for non-copyrighted-related reasons. On or about October 28, 2008, via Skype, VAN DER KOLK said to ORTMANN that TE "has declared the war on MRV already :)" because TE had "opened his own tube site, and started deleting his videos". It appears that TE was deleting his videos that had been uploaded to the Mega Sites. VAN DER KOLK then said, "so I banned him." Despite the deactivation, files that had been uploaded by TE continued to be distributed by members of the Mega Conspiracy for profit, without TE's consent. On or about August 14, 2008, DOTCOM forwarded an e-mail to VAN DER KOLK that had originally been sent by TE. In TE's original e-mail, TE stated that he planned to discontinue uploading to the Mega Sites, and that he wanted to have the right to delete all of the videos that he had stored on Mega's servers. In another e-mail sent on or about August 14, 2008, entitled "I want access to my videos!" TE stated that according to Megaupload's Terms of Service, uploaded videos belong to whoever uploaded them, not to Megaupload. DOTCOM forwarded the email to VAN DER KOLK and stated, "Do not turn this idiots account back on. And don't give him access to his videos." On or about December 13, 2008, TE e-mailed account@megaporn.com, stating that a video he had uploaded to the Mega Sites on November 7, 2007, was still available to the public, despite the fact that TE's account was deactivated.

*Inferences:* Mr Dotcom monitored the administration of the rewards scheme and was familiar with the cases of individual repeat infringers. He intended that Mega should benefit from the traffic to TE's infringing content, even to the extent of refusing to let TE remove videos he had uploaded.

[317] Paragraph [25h] shows another aspect of Mr Dotcom's involvement in the rewards scheme. In 2007 he drafted a press release for a variation in the rewards offered:

On or about December 2, 2007, DOTCOM sent an e-mail entitled "Feedback, opinions and improvements please!" to Ortmann, Van der Kolk, Bencko, and Echernach, with a draft press release regarding an "Xmas Special" for the "Uploader Rewards" program. In the e-mail, DOTCOM wrote:

For the whole month of December & January you will earn DOUBLE reward points for downloads of your files. Say good bye to the competition. Our Rewards program was already the best before this special. But now you must be crazy if you still upload to other sites :-)

Echternach responded with comments, and on or about December 3, 2007, DOTCOM ordered Bencko to "put the text I emailed first in the xmas special landing page and send me a link today. Also let me see the animated top and bottom."

*Inference:* Mr Dotcom was involved in the administration of the rewards scheme.

[318] In 2008, Mr Dotcom received an email from Warner Brothers identifying infringing content made available by AD and requesting that his account be suspended. Mega continued paying AD for his infringing content, from which it can be inferred that Mr Dotcom took no steps to have AD's content removed.

Paragraph [55]:

[...] on or about April 28, 2008, DOTCOM received an e-mail addressed to dmca@megaupload.com from Warner Brothers Entertainment identifying infringing content made available by AD and requesting that his account be suspended. Despite having received these takedown requests and this notification, the Mega Conspiracy never terminated AD and never purposefully and completely blocked access to the infringing content. Following the April 28, 2008 notification, AD continued to upload infringing content [...].

*Inference:* Mr Dotcom knew that repeat infringers were violating copyright but took no steps to ensure they were not paid rewards for doing so.

[319] In June 2011, shortly after the takedown of the Kino.to site, Mr Dotcom ordered the termination of the rewards scheme. He then drew attention to competitors by drawing PayPal's attention to their payment of rewards, which he described as "criminal" activity.<sup>87</sup>

*Inference:* Mr Dotcom knew the rewards scheme was operated in an unlawful manner, but took no steps to curb this aspect of Mega's copyright infringement until it seemed dangerous to continue.

*Mr Dotcom monitored the manipulation of free viewing time to maximise the purchase of subscriptions*

---

<sup>87</sup> Para [25j] [ROC bundle p 18-19).

[320] Most of the correspondence about the manipulation of viewing times was between Mr Ortmann and Mr van der Kolk, but several messages show Mr Dotcom closely watching this development.

[321] Paragraph [104o]:

On or about November 23, 2008, via Skype, ORTMANN and DOTCOM discussed whether the time limitation should be 60 or 72 minutes to maximize the number of users who decide to pay for premium membership. The conversation was originally in German. DOTCOM said, "MV is continuing to grow," "even with limits," and ORTMANN responded, "right." Later, DOTCOM said, "What I don't understand is why we don't do what we agreed on. 60 minutes playtime / 60 [minutes] waiting. I don't understand that. Isn't that what we agreed on?" ORTMANN responded, "Psychologically, I think it's better if people have to wait a little less than they are allowed to see in one go. We've more than reached the target payment level. We've continue to grow with real 72 Minutes. With real 60 Minutes, we are headed into new territory." ORTMANN also said, "Movies last 90 minutes. They're interesting in the last 20 minutes." Later, DOTCOM said, "Okay. It would just be nice if something like that got explained to me once in awhile. Just don't leave me in the dark. I had assumed 60 [minutes] here. Yesterday we said we would try it out for four days now WITHOUT screwing around. Instead, it's 72 [minutes] now. And yesterday, you had raised the limits for an hour again. That isn't what was agreed on. But it's no big deal. It would just be fair and proper if you would keep to agreements or at least clarify in advance any changes to agreements. I really wanted to see where the journey would lead with 60/60. And four days won't hurt anybody. MV will keep growing." ORTMANN responded, "No problem. We had identified 60 inexact Minutes as a sweet-spot. That it's 72 Minutes in reality - so much the better for the user. The sweet-spot attribute might completely have to do with the fact that movies heighten the suspense toward the end." DOTCOM asked, "But you yourself said that most of the movies with us are being uploaded in high bitrate?" and ORTMANN responded, "Low bitrate movies were really twice as long sometimes before the user got the message," "but long, low bit-rate movies [322] are rare (DVD rips are high quality)." In this context, the phrase "DVD rips" appears to refer to infringing copies of copyrighted DVDs.

[323] Paragraph [104p]:

On or about December 30, 2008, via Skype, ORTMANN told DOTCOM, in German, "What led to the miraculous MU turnaround at the end of July, we don't know. But the introduction of MV limitations was our most important, deterministic change in 2008."

*Inferences:* Mr Dotcom conspired with Mr van der Kolk and Mr Ortmann over the manipulation of free viewing limits, their object being to maximise the purchase of subscriptions. Mr Dotcom understood that the limits were calibrated to exploit the popularity of commercial copyright-protected movies.

*Mr Dotcom paid close interest in the activities of other officers*

[324] The applicant alleges that Mr Dotcom was not an aloof figure, far removed from the practical workings of the Mega business and he kept a close eye on the work of other officers.

[325] Paragraph [77a] and [77b]:

On or about April 27, 2009, DOTCOM sent an e-mail to VAN DER KOLK, ORTMANN, and co-defendant Julius Bencko ("Bencko"). In the email, DOTCOM wrote: "I want both of you [VAN DER KOLK and Bencko] to email me weekly detailed work reports. I want to know what you are currently working on and what tasks have been completed. I expect those emails every Friday."

On or about May 25, 2009, Nomm sent an e-mail to DOTCOM entitled "status report." In the e-mail, Nomm wrote, "Time for status report again." Nomm then provided a detailed description of software coding he had recently done for the Mega Sites. Nomm further wrote, "As always most of my current tasks info also Mathias [ORTMANN] has, we schedule and plan everything with him so he is up to date."

[326] Paragraph [170dd]. According to Mr Nomm:

DOTCOM personally negotiated with the largest Megaclck.com advertisers. BATATO dealt with advertisers and also supervised the salespeople who dealt with the other advertisers. When NOMM and BATATO disagreed whether an advertising campaign should be removed for violating the company's terms of service, ORTMANN would resolve the issue, with the ultimate authority being DOTCOM'S.

Paragraph [170bb]. Changes in certain advertising arrangements "would have to be approved by DOTCOM".

*Inference:* Mr Dotcom's role in the business meant that he inevitably knew of the extent of its copyright violations.

[327] The applicant says that Mr Dotcom's authority over the other members of the conspiracy is apparent from other evidence. The increase in Warner Brothers' daily quota for Abuse Tool link deletion was clearly a decision that required his involvement. The magnitude of Warner's deletion activities was a further indication of the scale of infringement on Mega sites.

Paragraph [31d]:

On or about September 4, 2009, a representative of Warner Brothers Entertainment, Inc. ("Warner"), sent an e-mail to Megaupload.com, stating that Warner was "unable to remove links" to copyright-infringing content on Megaupload.com using the Abuse Tool. In the e-mail, the Warner representative requested an increase in Warner's removal limit, which is controlled by the Mega Conspiracy. On or about September 8, the representative sent a follow-up request, and on or about September 9, the representative sent another follow-up request. On or about September 10, Ortmann sent an e-mail to DOTCOM, stating, "They are currently removing 2500 files per day - a cursory check indicates that it's legit takedowns of content that they own appearing in public forums." The term "public forums" likely refers to third-party linking sites. Ortmann also stated, "We should comply with their request - we can afford to be cooperative at current growth levels." DOTCOM responded that the limit should be increased to 5,000 per day, but "not unlimited", demonstrating that the Mega Conspiracy arbitrarily limited the ability of copyright owners to remove infringing content from the Mega Sites.

*Inferences:* Mr Dotcom made decisions about the rate of link deletions, which would potentially slow (but not prevent) traffic to infringing content. He was concerned to limit any loss of traffic rather than allow copyright owners to pursue "legit takedowns" to the full extent they could, albeit using the deceptive Abuse Tool.

[328] The applicant alleges that the decision to reinstate links to content identified by APCM, and to ignore takedown requests from countries outside the "first world", was driven by Mr Dotcom. Paragraph [133c 2], [133c 3] and [133c 5]:

Later that day, DOTCOM instructed ORTMANN, in German, "and please do what I wrote bram. undelete everything that was in the last 4 weeks reported from non first world countries. SIMPLY everything. And you will see we have daily record again."

Later that day, ORTMANN sent DOTCOM a portion of the APCM e-mail, which stated that APCM Mexico is the authorized representative of, amongst others, Columbia Pictures Industries, Inc., Disney Enterprises, Inc., Paramount Pictures Corporation, and Warner Bros. Entertainment Inc. ORTMANN told DOTCOM, in German, "if true, Bram has not done anything wrong." A few minutes later, DOTCOM blamed the takedowns for causing "50k revenue gone."

Later that day, DOTCOM told VAN DER KOLK and ORTMANN: make a list of all links that were reported from mexico, brazil, and other non first world countries in the last 4 weeks. and undelete all of them. They have not sent us legitimate takedown notices with sufficient proof that they represent the right holders for every single link. and from now on you will only delete links from the USA, France, Germany, UK and SPAIN instatntly.

*Inferences:* Mr Dotcom made decisions about the extent to which Mega would comply with its copyright law obligations. Although Mr Ortmann and Mr van der Kolk had a different view about the risk of ignoring takedown notices from these sources, they were not willing to disobey Mr Dotcom. Mr Dotcom's concern was to maintain traffic volumes by frustrating the efforts of copyright owners to protect their interests.

*Mr Dotcom communicated with other officers in ways that showed knowledge the Mega sites hosted significant infringing content*

[329] Paragraph [38l]:

On or about May 25, 2009, NOMM sent an e-mail to DOTCOM and Ortmann entitled "status report." Nomm wrote, "I have been processing HD videos for some time now to find best of the best for showcase (Mathias gave specification). Even though we have lots of HD content uploaded most seems to be problematic quality or legality wise." The term "HD" refers to high definition content.

Paragraph [38o]:

On or about September 5, 2010, Bencko sent an e-mail to DOTCOM, Ortmann, and Van der Kolk. Attached to the e-mail message was a screenshot of Bencko logged into a Megaupload.com file download page with a filename of "Meet.Dave.2008.avi". "Meet Dave" is a copyrighted motion picture.

Paragraph [103q]:

On or about November 14, 2007, via Skype, DOTCOM said to ORTMANN, in German, "will you eventually solve the conversion problem? the complaints don't stop. what do you think you can do?" ORTMANN responded, "we have a long queue of dvd-rips" "and some DRM protected, that cannot be converted." DOTCOM replied, "then we need more conversion servers", "please order." The acronym "DRM" refers to "Digital Rights Management" and is commonly understood to mean copyright-protection based in either software, such as encryption, or somewhat less commonly, hardware. During that time period, the Mega Conspiracy was converting user-uploaded videos, including copyrighted videos, into a particular video format known as Flash Video or "FLV," which facilitated the video's distribution.

Paragraph [103oo]:

On or about March 20, 2009, via Skype, DOTCOM and ORTMANN discussed providing high definition content on Megavideo.com. DOTCOM said, in German, "I'm looking forward to MV [HD,]" "it will be cool." ORTMANN responded, "The quality is going to be amazing ... the Warner Brothers opening credits for Terminator 3 on Andrus' [NOMM] unoptimized

demo video is already a feast for the eyes.” “Terminator 3: Rise of the Machines” is a copyrighted motion picture.

Paragraph [148e]:

Throughout the Mega Sites' existence, the websites had a difficult time attracting legitimate advertisers because advertisers were concerned about being associated with a website that facilitated the reproduction and distribution of copyright-infringing materials. Advertisers and others regularly shared these concerns with defendants.

i. On or about March 26, 2011, via Skype, DOTCOM asked BATATO in German, "How are things going with the new sales team?" BATATO answered, "So so. The US-boys are being difficult because the Media agencies pick on the Content License Topics. Will get together with the ad tech folks and see how we can approach the market better."

ii. On or about July 28, 2011, via Skype, BATATO said to DOTCOM in German, "Essentially we are seeing an increase of concerns in regards to Copyright/DMCA."

iii. On or about September 29, 2011, via Skype, ORTMANN told DOTCOM in German that the "Australian mobile aggregator" was shutting down Megaupload in Australia. DOTCOM responded, "ozzies, just as dumb as the kiwis." ORTMANN replied, "hehe."

Paragraph [148f]:

On or about October 6, 2010, via Skype, ORTMANN sent DOTCOM a link to the agenda for the 2010 International Law Enforcement IP Crime Conference, which was co-hosted by Interpol and Hong Kong Customs and located at the Hong Kong Grand Hyatt Hotel, the Mega Sites' headquarters. ORTMANN commented in German, "in the lion's den."

*Inferences:* Mr Dotcom and the other respondents deliberately ran the business in ways that injured the rights of copyright owners. They were aware of Mega's reputation for copyright piracy.



*Mr Dotcom was aware of the extremely high numbers of takedown notices directed at content hosted by Mega.*

[330] Paragraph [77d]:

E-mails sent to a number of accounts associated with the Mega Sites were forwarded to DOTCOM. Between at least June of 2007 and February of 2008, DOTCOM received more than 400,000 e-mails addressed to paypal@megaupload.com, which consisted primarily of notifications of payments received by the Mega Sites through PayPal. Between at least June of 2007 and August of 2008, DOTCOM received more than 180,000 emails addressed to abusereport@megaupload.com, which consisted primarily of copyright-infringement and other takedown notices. Between at least June of 2007 and December of 2011, DOTCOM received more than 280,000 e-mails addressed to abuse@megaupload.com, which consisted primarily of copyright-infringement and other takedown notices. Between at least June of 2007 and August of 2008, DOTCOM received more than 80,000 e-mails addressed to or sent from support@megaupload.com which consisted primarily of requests for user support, notifications of account suspensions, and notifications associated with the Uploader Rewards program. Between at least June of 2007 and December of 2011, DOTCOM received more than 80,000 e-mails addressed to [legal@megaupload.com](mailto:legal@megaupload.com), which consisted primarily of copyright-infringement and other takedown notices. Between at least August of 2007 and December of 2011, DOTCOM received more than 79,000 e-mails addressed to abuse@megavideo.com, which consisted primarily of copyright infringement and other takedown notices. Between at least June of 2007 and December of 2011, DOTCOM received more than 30,000 e-mails addressed to sales@megaupload.com, which consisted primarily of correspondence from third-party businesses. Between at least June of 2007 and December of 2011, DOTCOM received more than 20,000 emails addressed to hq@megaupload.com, which consisted primarily of e-mails associated with DOTCOM's role as the Chief Executive Officer of the Mega Sites. Between at least August of 2007 and April of 2009, DOTCOM received more than 20,000 e-mails addressed to dmca@megavideo.com, which consisted primarily of copyright-infringement and other takedown notices. Between at least November of 2008 and December of 2011, DOTCOM received more than 8,000 e-mails addressed to abuse@megaporn.com, which consisted primarily of copyright-infringement and other takedown notices. Between at least February of 2009 and December of 2011, DOTCOM received hundreds of e-mails addressed to leagl@megaporn.com, which consisted primarily of copyright-infringement and other takedown notices.

*Inference:* Mr Dotcom knew that Mega was hosting a very large number of infringing files, which copyright owners were detecting in publicly accessible sites on the Internet.

*Mr Dotcom monitored the appearance of Mega sites and ensured they maintained a sanitised appearance*

[331] The applicant alleges Mr Dotcom was involved in the sanitised “Top 100” list of Mega downloads. Paragraph [30a]:

On or about July 18, 2008, DOTCOM received an e-mail from a web designer, regarding the development of the Megaupload.com "Top 100." That same day, DOTCOM forwarded the e-mail to Ortmann and Van der Kolk, writing: "Number 1 download will of course be Mega Manager :-)".

Paragraph [148c]:

As referenced in Paragraphs 18 and 30 of the Record of Case, the defendants made Megavideo's front page appear more legitimate by screening out copyright-infringing content, in particular from the Top 100 list. After such content was eliminated, however, there was apparently so little remaining content that on or about December 21, 2011, via Skype, DOTCOM told VAN DER KOLK, "i need someone to implement the reupload logic we discussed some time ago. it is not good whats happening now with videos on the first page listed as uploaded 2 days ago." VAN DER KOLK responded, "Okay, I will try to come up with something for that asap." DOTCOM then instructed VAN DER KOLK, "just reupload everything from 2 years ago in the same order. same user names, everything[,] and mingle with the new uploads." VAN DER KOLK responded, "Yes sir, will do that."

Paragraph [103ss]:

On or about November 19, 2009, via Skype, DOTCOM sent ORTMANN a Skype conversation between DOTCOM and VAN DER KOLK, during which DOTCOM said:

MV is full of problematic content on the [publicly viewable] video pages. I told you how important this is. Every day counts, especially since we have articles out there comparing us with napster and putting us in a bad light. WHY THE FUCK did you not take care of this? You told me you will do this WHILE you are in HK. I just spoke with mathias [ORTMANN] and he told me he informed you long time ago about fixing this. WHY do you risk our good running business with not following up on important matters like this. If you look at the latest video pages now it is FULL with the latest commercial stuff. FUCK THIS BRAM! [...].

*Inference:* Mr Dotcom conspired with Mr Ortmann and Mr van der Kolk to disguise the availability of copyright infringing content on Megaupload and Megavideo.

*Mr Dotcom's role in the mass acquisition of YouTube videos*

[332] There is one message in which Mr Dotcom's supervision of the YouTube infringement is made clear by his own statement. Paragraph [105i]:

On or about October 4, 2007, via Skype, VAN DER KOLK sent to ORTMANN a conversation between VAN DER KOLK and DOTCOM, where DOTCOM stated, “the day has 1440 minutes and I want to see one Video upload on megavideo every minute. If necessary use the youtube videos we still have unpublished and publish one by one from dirrent accounts every minute,” and “otherwise we look like small fish shit.”

*Inference:* Mr Dotcom conspired with Mr Ortmann and Mr van der Kolk to disguise the availability of copyright infringing content on Megavideo.

Paragraph [74e]:

According to internal e-mails and documents obtained from Google, members of the Mega Conspiracy, including DOTCOM and VAN DER KOLK, began accessing Google Analytics reports for Megavideo.com, Megaupload.com, and Megaporn.com. The Google Analytics account was opened at least as early as November of 2008 under the name "TIM VESTOR," which is an alias for DOTCOM. Google Analytics provides website measurement tools, such as the number of visits during a specified time period.

1. A particular Google Analytics report shows that between November 19, 2010, and February 18, 2011, Megavideo.com had roughly 1 billion visits. Less than 13% of these visits were "direct traffic" — meaning visits that were likely generated by the user having directly typed the URL link into the web browser or having bookmarked the URL link. More than 85% of the visits to Megavideo.com were from "referring sites," meaning the user appears to have clicked a URL link on the referring site that directed the user to Megavideo.com. The top referring websites during that time period were third-party linking sites, such as seriesvonkis.com (more than 110 million referrals) and sidereel.com (more than 60 million referrals). The reports from Google Analytics for the following time periods reflect similar data: February 19, 2011 — May 18, 2011; May 19, 2011 — August 18, 2011; August 19, 2011 — October 27, 2011.

2. A particular Google Analytics report shows that between November 19, 2010, and February 18, 2011, Megaupload.com had roughly 1 billion visits. Less than 20% of these visits were "direct traffic," and roughly 80% were from "referring sites." The top referring websites during that time period were third-party linking sites, such as taringa.net (more than 50 million referrals), seriesvonkis.com (more than 25 million referrals), and multiupload.com (more than 20 million referrals). The reports from Google Analytics for the following time periods reflect similar data: February 19, 2011 — May 18, 2011; May 19, 2011 — August 18, 2011; August 19, 2011 — October 27, 2011.

And, at paragraph [132 a]:

eXTReMe digital V.O.F. (“Extreme Tracking”), a Dutch company, provides website measurement tools, such as the number of visits during a specified time period. These tools are available at the website ExtremeTracking.com. According to records provided by Extreme Tracking, as early as May of 2005, the Mega Conspiracy opened 4 separate analytics accounts under the name

“KIMBLE,” which is an alias for DOTCOM. These analytics accounts tracked the websites Megavideo.com, Megaupload.com, Megaporn.com, and Sexuploader.com.

Paragraph [130d 3]:

On or about February 3, 2009, via Skype, DOTCOM told ORTMANN, in German, “MV has 1 million less users on Extreme Tracking since the removal of watch-movies[.net]. But strangely, this has no effect on payments. Really funny.”

[333] The applicant says that throughout the Mega sites’ existence, discussions between Mr Dotcom and the other respondents reflect the fact that they viewed the Mega sites’ competitors as other websites that facilitated the reproduction and distribution of copyright-infringing materials, as opposed to legitimate storage locker sites.

Paragraph [148d]:

i. On or about July 4, 2010, via Skype, DOTCOM and ORTMANN in German, discussed a competitor’s website, Hotfile.com (“Hotfile”). DOTCOM said, “we . . . need to improve our reward system. Unfortunately hotfile is pulling past us right now.” He added, “we should just lie a little about the rewards, just like hotfile.” ORTMANN responded, “we are already lying...we just have to lie some more.” DOTCOM replied, “hehe.” ORTMANN then said, “if we truthfully paid our rewards, we would have more than 500k extra expenses a month.” DOTCOM responded, “wow.” On or about December 4, 2013, Hotfile ceased all operations, the same day it signed an \$80 million settlement with the Motion Picture Association of America (“MPAA”) in relation to Hotfile’s reproduction and distribution of copyright-infringing material.

ii. On or about August 16, 2010, via Skype, DOTCOM and ORTMANN, in German, discussed a competitor’s website, Rapidshare.com (“RS”). ORTMANN noted that “the RS-graph on Google Trends looks depressing (for RS).” Shortly thereafter, ORTMANN added that Megaupload’s “fall growth will be similar to last year, due to the outage of RS it will probably be more extreme.” In other words, the Mega Sites stood to gain Rapidshare’s users. On or about October 22, 2010, via Skype, DOTCOM told ORTMANN, in German, that uploads and payments “have exploded.” ORTMANN responded, “yep, migration from RS.” On or about September 22, 2011, via Skype, ORTMANN told DOTCOM, in German, regarding the “rapidshare—spillover from last year,” that “we are spilling over to aggressive inducers.” In the context of this discussion, it appears that ORTMANN was raising a concern that other websites (i.e. “aggressive inducers”) were attracting the Mega Sites’ users because they were offering more aggressive rewards at the time. In approximately March 2012, the Hamburg higher regional court upheld three earlier decisions finding that Rapidshare could be held liable for publication of copyright-protected material by third parties.

## Paragraph [148g]:

Throughout the Mega Sites' existence, the defendants discussed their knowledge of, and reliance on, specific third-party referrer websites. For instance, on or about September 16, 2011, via Skype, DOTCOM asked ORTMANN in German why the Mega Sites recently experienced a "sharp decline" in traffic. ORTMANN responded by discussing Megaupload's third-party linking sites and explained, "the only referrer with major movement is taringa — they cut from one day to the next 50%, although that was the beginning of May. All other referrers are unchanged. . . . I am currently with the uploader analysis — not every referrer shows up as a referrer, many no longer link directly."

## Paragraph [149]:

a. As described in Paragraph 132 of the Record of the Case eXTReMe digital V.O.F. ("Extreme Tracking"), a Dutch company, provides website measurement tools, such as the number of visits during a specified time period. These tools are available at the website ExtremeTracking.com. According to records provided by Extreme Tracking, as early as May of 2005, the Mega Conspiracy opened 4 separate analytics accounts under the name "KIMBLE," which is an alias for DOTCOM. These analytics accounts tracked the websites Megavideo.com, Megaupload.com, Megaporn.com, and Sexuploader.com.

b. As described in Paragraph 132 of the Record of the Case, visitors searching for terms specific to copyrighted works were referred to the Mega Sites on a daily basis. The searches described in Paragraph 132 included searches done through Google.com, amongst other online search engines.

c. DOTCOM's Internet browsing history revealed that he had visited the Extreme Tracking website at least approximately 100 times, including but not limited to September 25, 2011 and October 31, 2011. Extreme Tracking analytic reports showed that several of the websites that referred traffic to Megaupload.com and Megavideo.com provided specific links to copyright infringing content. The September 25, 2011 analytic report, for example, showed that the link [egsoftwares.blogspot.com/2010/04/nballersphenomps2.html](http://egsoftwares.blogspot.com/2010/04/nballersphenomps2.html) referred traffic to Megaupload.com. This link appears to advertise the copyrighted video game "NBA Ballers Phenom" for the Sony PlayStation 2 video game console. Another report on that same date showed that the link [como-conoci-a-vuestramadre.seriespepito.com/capitulosquinta-temporada-5/capitulo-24-doppelganger/](http://como-conoci-a-vuestramadre.seriespepito.com/capitulosquinta-temporada-5/capitulo-24-doppelganger/) referred traffic to Megavideo.com. This link, translated from Spanish, refers to the copyrighted television series "How I Met Your Mother."

*Inferences:* Messrs Dotcom, Ortmann and van der Kolk shared knowledge that traffic flows to Mega sites were primarily via linking sites to copyright infringing content. Traffic might be influenced by the fortunes of sites specialising in the provision of access to infringing content.

[334] The applicant alleges that Mr Nomm confirms:

- (1) He and each of the co-conspirators periodically discussed the fact that users often discovered copyright-infringing content stored on the Mega Sites through third-party linking sites. This must include discussions involving Mr Dotcom.<sup>88</sup>
  
- (2) The respondents were aware they were making money directly from reproducing and distributing copyright-infringing content uploaded to the Mega sites. This included millions of dollars made from advertisements posted on the Mega sites through Megaclick.com.<sup>89</sup> Mr Dotcom personally negotiated with the largest Megaclick.com advertisers and involved himself with the practical running of the Megaclick side of the business. This included changes to the format of advertising that resulted in the insertion of ads directly within videos, “including, inevitably videos that were copyright-infringing”.<sup>90</sup>

*Mr Dotcom concerned himself in the media image of the Mega business.*

[335] Paragraph [38m]:

On or about October 3, 2009, DOTCOM sent an email entitled "FWD: Re: Reporter hoping to speak about copyrighted content on Megavideo" to an employee and to Ortmann containing a series of statements purportedly from "[BL], Public Relations, Mega HQ" to a reporter for Forbes.com. In DOTCOM's original e-mail to his employee, he informs her that "I used your name in the emails below. I hope you don't mind. Please be careful. The larger we get the more people want to know more about Mega. Lets stay below the radar." The Forbes.com reporter had asked about KIM SCHMITZ and TIM VESTOR's role in the company. DOTCOM wrote in response, "I can confirm that nobody by the name of Kim Schmitz is associated with our company." DOTCOM further tells the reporter "We have a policy not to disclose details about our business performance. But I can tell you (off the record) that we are a small and humble business trying to earn enough to pay the bandwidth bill. Our site has grown to be popular but it is not easy to monetize the traffic in this economy." DOTCOM also indicates, "The vast majority of users is uploading home videos, web cam captures, content they own or have the right to copy and other legitimate content".

[336] Paragraph [38q]:

---

<sup>88</sup> SROC 6 para [170m] (ROC bundle p 310).

<sup>89</sup> SROC 6 para [170n] (ROC bundle p 310).

<sup>90</sup> SROC 6 para [170bb], [170cc], [170dd], (ROC bundle p 313).

On or about January 13, 2011, DOTCOM sent a proposed Megaupload.com public statement regarding piracy allegations against the website to hosting company executives DS and JK. On or about January 13, 2011, DS replied to DOTCOM: "It looks accurate to me, good luck." The same day, JK replied, "Using the words, `...vast majority is legitimate.' Opens you up. It's an admission that there are 'bad' things on your site. I would get rid of that so it simply reads that it is legitimate."

*Inference:* Mr Dotcom was involved in practical ways with the management of the business and was particularly concerned to disguise the extent of its copyright violations.

*Mr Dotcom dealt with corporate concerns about piracy on Mega sites*

Paragraph [38e]:

On or about May 17, 2007, a representative from Google AdSense, an Internet advertising company, sent an e-mail to DOTCOM entitled "Google AdSense Account Status." In the e-mail, the representative stated that "[d]uring our most recent review of your site [hkgupload.com,]" Google AdSense specialists found "numerous pages" with links to, among other things, "copyrighted content," and therefore Google AdSense "will no longer be able to work with you." The e-mail contains links to specific examples of offending content located on Megaupload.com.

Paragraph [38p]:

On or about November 1, 2010, Echternach forwarded an e-mail from a Universal Music Group ("UMG") executive to DOTCOM and Ortmann, which discussed requirements that UMG would require of Megaupload before they could discuss licensing for MegaBox, a music-hosting service allegedly being developed by the Mega Conspiracy. Included in the list of requirements was "proactive fingerprint filtering to ensure that there is no infringing music content hosted on its service; proactive text filtering for pre-release titles that may not appear in fingerprint databases at an early stage; terminate the accounts of users that repeatedly infringe copyright; limit the number of possible downloads from each file; process right holder take down notices faster and more efficiently."

*Inference:* In the course of his involvement with the business, Mr Dotcom was obliged to confront concerns about piracy on Mega sites.

[337] The applicant alleges that a credit card payment processor conveyed complaints from copyright holders and this was brought to Mr Dotcom's attention. His disingenuous response ignored the financial benefits Mega obtained from giving

access to popular copyright material. It also ignored Mega's obligations to deal with repeat infringers.

Paragraph [38d]:

On or about December 11, 2007, a credit card payment processor e-mailed Echternach and Van der Kolk regarding "complaints" that the processor had received from third-parties involving copyright-infringing materials found on the Mega Sites, including one complaint in which a third-party stated: "we have pulled over 65 full videos from Megarotic. That's \$200k in content we paid for." In the e-mail to Echternach and Van der Kolk, the processor stated, among other things: "you are not allowed to sell or financially benefit from the content that is infringing in copyrights on your site"; and "you are not allowed to continue with allowing the user to upload content if you can have knowledge of the infringing of copyright." DOTCOM responded to the e-mail, stating "The DMCA quotes you sent me are not relevant. We are a hosting company and all we do is sell bandwidth and storage. Not content. All of the content on our site is available for 'free download'."

*Inference:* Mr Dotcom's management of the business was characterised by a determination to persist with copyright infringing activities.

[338] The applicant alleges that although Mr Dotcom was well aware of DMCA requirements to deal with repeat infringers, he did nothing to curb their activities and payments to reward claimants did not cease until June 2011.

Paragraph [38t]:

On or about February 18, 2011, DOTCOM forwarded an e-mail inquiry entitled "'Repeat Offender' Infringement Policy" to Ortmann. In the original e-mail, a representative of a copyright holder indicates that Megaupload.com does not specify any "repeat offender or repeat infringer policy" in its Terms of Service. The representative points out that the "Safe Harbor" provision of the DMCA "requires that providers deal appropriately with repeat offenders" and asks for the termination of repeat offenders on Megaupload.com. As demonstrated in the sections entitled Willful Failure to Remove Copyright-Infringing Files and Misrepresentations to Copyright Owners, the Mega Conspiracy failed to terminate repeat infringers.

*Inference:* Mr Dotcom sought to profit from the activities of repeat infringers and ran the business in ways that avoided its legal obligations to curb copyright infringement.

[339] The applicants allege that Mr Dotcom was also involved in the deception of copyright owners. At paragraph [152], he told Universal Music Group that Mega removed "content swiftly":



Paragraph [152]:

The U.S. Attorney's Office for the Eastern District of Virginia expects a representative of the FBI to testify that during a conversation between DOTCOM and a representative of Universal Music Group that occurred on or about January 18, 2012, a recording of which was discovered on DOTCOM's iPhone, DOTCOM told the representative, "We remove content swiftly." Despite DOTCOM's claim that "content" had been "remove[d]" from the Mega Sites, the Mega Conspiracy merely disabled specific URL links identified in copyright takedown notices and did not remove the underlying infringing content, which continued to be reproduced and distributed through the Mega Sites.

*Inference:* Mr Dotcom deceived copyright owners about the action Mega took in response to takedown notifications.

[340] The applicant alleges that Mr Dotcom involved himself in other attempts to mask the real nature of Mega's operations. Soon after the cessation of the rewards scheme, Mr Dotcom wrote to Paypal highlighting the "criminal activities" of rival companies, but neglecting to say that Mega had done the same things until recently. It submitted that it is a reasonable inference that he knew and approved of Mr Ortmann's attempt to have the USTR remove Megaupload from its Notorious Market List, which involved a number of false representations about its response to copyright infringement. The need to provide such false explanations is consistent with knowledge that these aspects of the business's operations were unlawful.

*Mr Dotcom monitored legal threats to the Mega business*

[341] Paragraph [38n]:

On or about July 8, 2010, DOTCOM sent an e-mail to Ortmann and Echternach entitled "attention." In the e-mail, DOTCOM copied a link to a news article entitled "Pirate Bay and Megaupload Escape Domain Seizure by US." The article discussed how, "[a]s part of an initiative to crack down on Internet piracy and counterfeiting, the US Government recently took action against sites making available movies and TV shows." In addition to the link to the article, DOTCOM wrote, in full:

this is a serious threat to our business. Please look into this and see how we can protect ourselves. Is everything regarding our domain records now 100% in order? Should we move our domain to another country (canada or even HK?) Suggestions, please.

Echternach responded: "In case domains are being seized from the registrar, it would be safer to choose a non-US registrar [.]"

Paragraph [38r]:

On or about February 5, 2011, Ortmann responded in an e-mail to DOTCOM, copying Echternach and Van der Kolk, about an article that DOTCOM sent him entitled "how-to-stop-domain-names-being-seized by the-us-government." Ortmann indicates the status of the Mega Conspiracy's completion of the recommendations made in the article.

Paragraph [38w]:

On or about October 10, 2011, JK, an executive from a hosting provider, sent an e-mail to Ortmann entitled "Article." The e-mail contained a link to a news article, which discussed how a Dutch court ordered a "major" website "to delete all infringing content from its servers." The article asked: "Could file-hosting services like MegaUpload and RapidShare be next?" In the e-mail, JK asked Ortmann: "Do you have any concerns that this kind of thing could find its way to you"? Ortmann responded to JK, with a copy to DOTCOM, stating that the sites in the article "provide a search index covering their entire content base, including the infringing material." As described above, Megaupload.com did not provide any search index whatsoever to the public, but had an internal index that reveals many hundreds of thousands of copyright-infringing works on the Mega Sites.

Paragraph [103jj]:

On or about March 8, 2009, via Skype, DOTCOM asked ORTMANN, in German, "Have you got a minute? Let's talk about how we should prepare for lawsuits, should they ever happen." ORTMANN responded, "We need to take a look at how YouTube has dealt with that so far. Promise some kind of technical filtering crap and then never implement it." DOTCOM added, "We should already be hiring an attorney now, perhaps an in-house one, to get us prepared for anything."

[342] The applicant says that Mr Dotcom foresaw that Mega might lose server capacity through court orders and wanted to mitigate that risk by owning its own servers in a number of countries.

Paragraph [148b]:

On or about August 16, 2010, via Skype, DOTCOM told ORTMANN in German, "at some point a judge will be convinced about how evil we are and then we're in trouble. We have to make ourselves invulnerable." To prevent this possibility, DOTCOM suggested "a new hosting model" that would make Megaupload "independent from," its server hosting facilities, "Capathia or leaseweb." DOTCOM said that Megaupload "should set up a fleet of our own servers with multiple hosters (15 or more in several countries) and make us untouchable." DOTCOM was particularly concerned about the domain name, stating, "The domain is the only danger, but for that there is the megakey." ORTMANN responded, "to counter the justice system with technical methods

is difficult at our size . . . a piratepay places a few GB backup on new servers and is back online, with 30+ PB that's a little more difficult." In this context, the acronym "PB" refers to petabytes of data. DOTCOM replied, "the file servers are not the issue here. The web and db servers are. This structure has to be secure." DOTCOM added, "none will impound 1000 file servers." ORTMANN responded, "as soon as the laws change, we will not survive with technical methods." ORTMANN also said, "if a US-court prohibits Cogent from providing us service, we will soon lose the vast majority of our connectivity worldwide." DOTCOM then reminded ORTMANN, "you should not log our chats ;-)" too much shit in there." ORTMANN responded, "unfortunately Skype autologs them . . . I'm going to erase them all."

Paragraph [148d iii]:

As discussed in Paragraph 100 of the Record of the Case, the company Perfect 10 Inc. filed a civil lawsuit against Megaupload Limited and DOTCOM, which the parties settled in October of 2011. On or about January 5, 2012, via Skype, in German, DOTCOM proposed to ORTMANN that they finance the Perfect 10 legal team "to go against several competitors such as filesonic and fileserve, then split up the settlement payment 50/50." DOTCOM then said, "if we could convince him [the legal team] to tame ou[r] toughest competition, that would be good for us." ORTMANN responded that "we should not participate at all . . . we will just be in a position of being blackmailed . . . Even if he just threatens us to forward the emails to torrentfreak." In approximately January of 2012, shortly after the arrest of the Mega Defendants and shut down of the Mega Sites, both Fileserve and Filesonic ceased offering file sharing services. FileSonic posted on its website a message stating: "All sharing functionality on FileSonic is now disabled. Our service can only be used to upload and retrieve files that you have uploaded personally."

*Inferences:* Dotcom appreciated that the extent of Mega's copyright infringements exposed it to the risk of legal action. His exchanges with Mr Ortmann show a determination to continue operating unlawfully in the face of any action that copyright owners or a court might take against Mega.

[343] It is alleged that Megaupload and Megavideo did not provide service to Internet Protocol addresses associated with Hong Kong. Mr Batato explained in several communications that the reason was to avoid the risk from legal actions in the state where these Mega companies were registered.<sup>91</sup> The decision to block Hong Kong traffic must have been within Mr Dotcom's knowledge and is consistent with his appreciation that Mega would inevitably face legal action because of its systematic copyright infringement.

---

<sup>91</sup> SROC 5 para [165] ROC para [39I]. (ROC bundle pp 281, 40).

*Mr Dotcom knew that users visited Mega sites to access infringing content*

[344] The applicant alleges that the following examples highlight that Mr Dotcom was aware that the Mega sites were primarily used for accessing and distributing copyrighted material.

Paragraph [38f]:

On or about June 30, 2008, abuse@megaupload.com received an e-mail entitled "illegal links", in which the author wrote that Megaupload.com "is being used for violations of copyright material in video." The author was not identified as a copyright owner, but the author listed over one hundred and thirty URL links to "illegal content" on Megaupload.com. On or about July 1, 2008, DOTCOM forwarded the message to Ortmann and Van der Kolk, instructing them: "Never delete files from private requests like this. I hope your current automated process catches such cases."

Paragraph [38h]:

On or about November 17, 2008, DOTCOM forwarded an e-mail to Ortmann from a customer that indicated: "I just want to start of by saying that i love the site, but today i discovered something i would consider a flawd. I was watching a video of Myth Busters when i recived a message that said 'You have watched 3079 minutes of video today'. Ortmann responded to DOTCOM that this was the correct behavior of the service. "MythBusters" is a copyrighted television series on the Discovery Channel."

Paragraph [38v]:

On or about August 11, 2011, DOTCOM forwarded an e-mail to Ortmann from a user who stated: "I used to buy monthly fees to help with the cost of you guys doing business . I miss being about to view tv shows on you service . My most favorite was True blood and battle star Gallactica . would be happy to continue to pay for the service , but some thing would needs to change. I don't mind your services be bogged down from time to time. I don't mind paying, but i need to get something for the service I pay for." "True Blood" is a copyrighted television series on the premium channel Home Box Office. "Battlestar Galactica" is a copyrighted television series that originally aired on the Sci-Fi Channel.

Paragraph [38i]:

On or about November 23, 2008, DOTCOM forwarded an e-mail to Ortmann and Echternach from a non-premium customer that indicated "I guess we need to find a new hobby because watching pirated material via megavideo is now over-rated and ruined because of this video bandwidth limit".

Paragraph [33d]:

On or about November 23, 2008, DOTCOM received an e-mail from a Mega Site user entitled "video problems." The e-mail described, "I've been trying to watch Dexter episodes, but. the sound doesn't match up with the visual... I didn't choose to use your site, you seem to dominate episodes 6 and 7 of Dexter on alluc[.org, a linking site]." DOTCOM forwarded the email to Ortmann and wrote, "... on many forums people complain that our video / sound are not in sync... We need to solve this asap!" "Dexter" is a copyrighted television series on the premium cable channel Showtime.

Paragraph [38s]:

On or about February 10, 2011, DOTCOM forwarded a complaint to Ortmann from a Taiwanese broadband service provider about problems its users have had downloading from Megaupload.com. In the screenshots that are in the original e-mail complaint is what appears to be an ongoing download of a copyrighted The Simpsons episode from Fox Television entitled "Treehouse of Horror XIII." In the e-mail, the representative of the Taiwanese broadband service provider wrote, "All the IPs have the same routing path from [the Taiwanese broadband service provider] to megaupload servers[.]" The screenshots, which are clearly visible in the email, visually demonstrate the download path taken by the downloaded file, from the provider's connection to Cogent to the Mega Conspiracy's servers.

[345] Paragraph [170x] describes Mr Nomm's experience of receiving, via Mr van der Kolk, emails from users who had problems viewing videos on Mega sites. He found many of the videos were copyright infringing videos and television programmes. "[N]umerous files that were hosted on the Mega Sites contained the "FBI Anti- Piracy" warning. Mr Nomm specifically advised Mr Dotcom and Mr Ortmann about the legality of the files being hosted", an assertion confirmed by paragraph [38l].

Paragraph [203y] says:

On or about June 15, 2008, via Skype, DOTCOM told ORTMANN, in German, "we should really focus massively stronger on anime there" because "they really rip everything." He added, "we have a real chance here to build a super advertisement machine." In this context, the term "rip" meant to reproduce the material in a manner that infringed copyright.

*Inferences:* Mr Dotcom appreciated that users accessed infringing content on Mega sites. He deliberately ran the business to capitalise on traffic to infringing content and was unconcerned by illustrations of such activity.

*Mr Dotcom knew the sites held infringing materials and personally accessed them*

Paragraph [38e]:

On or about December 12, 2007, Batato distributed a Megaupload.com link to an infringing copy of the copyrighted music file "Louis Armstrong — We have all the time in the world.mp3" to DOTCOM. An infringing copy of this copyrighted work was still present on servers leased by the Mega Conspiracy as of September 2, 2011.

Paragraph [103b]:

On or about February 2, 2007, via Skype, VAN DER KOLK sent ORTMANN a URL link to the copyrighted song "Kiss Me" by Sixpence None the Richer, which had been uploaded to Megaupload by an anonymous user. ORTMANN then forwarded the URL link to DOTCOM.

Paragraph [103c]:

On or about February 7, 2007, via Skype, ORTMANN sent DOTCOM a URL link to the copyrighted computer software Microsoft Windows XP, which had been uploaded by a registered Megaupload user.

Paragraph [150:]

The U.S. Attorney's Office for the Eastern District of Virginia expects a representative of the FBI to testify that DOTCOM's laptop contained a file entitled, "site\_megaupload.com The Beatles\_ - Google Search.pdf." The 26-page PDF document contained the Google search results for the following query: "site:megaupload.com `The Beatles'". The Google search returned more than 200 unique Megaupload.com URLs to files that were labelled, described, or associated with the phrase "The Beatles." A preliminary analysis of the Megaupload database showed that as of January 20, 2012, at least 11 of these URLs were still active.

Paragraph [153]:

The U.S. Attorney's Office for the Eastern District of Virginia expects a representative of the FBI to testify to the following facts:

a. DOTCOM's external hard drive contained at least 35 sound recordings, whose MD5 hashes matched those of files that had been uploaded to the Mega Sites. These sound recordings included the following:

- i. "Phone Tap" performed by The Firm.
- ii. "ATLiens" performed by OutKast.
- iii. "I Need Love" and "Rock the Bells" performed by LL Cool J.
- iv. "Smoke BUddah" performed by Redman.
- v. "Guess Who's Back" performed by Rakim.
- vi. "Money, Cash, Hoes," performed by Jay-Z.

- vii. "Ready or Not" performed by The Fugees.
- viii. "The Hard Way", "Rhyme the Rhyme Well", "Triple Trouble", "Oh Word?", "All Lifestyles", and "The Brouhaha" performed by Beastie Boys.
- ix. "Imagine" performed by John Lennon.
- x. "Let it Be", "Revolution", "Strawberry Fields Forever", "Yellow Submarine", "Yesterday", and "Lucy in the Sky with Diamonds" performed by the Beatles.
- xi. "Rock Your Body" performed by Justin Timberlake.
- xii. "Get The Party Started" performed by Pink.
- xiii. "Little L", "Virtual Insanity", and "You Give Me Something" performed by Jamiroquai.
- xiv. "My Interpretation", "Love Today", "Any Other World", "Billy Brown", "Big Girl (You Are Beautiful)", and "Happy Ending" performed by Mika.
- xv. "Say It Right" performed by Nelly Furtado.
- xvi. "Will You Still Love Me?" performed by Chicago.
- xvii. "Along Comes Mary" performed by Bloodhound Gang.

[346] The applicant alleges that these files infringed copyright. See para [154] of SROC 4. Para [163] of SROC 5 explains further that the files “were not found in Mr Dotcom’s identified Megaupload accounts.” The inference this supports is that Mr Dotcom had not uploaded these files himself, but had located them on Mega sites and downloaded them to his hard drive. In other words, these were not private backups but infringing downloads.

Paragraph [77c]:

[347] DOTCOM maintained a number of active accounts on the Mega Sites. One of his Megaupload.com accounts contained an infringing copy of the copyrighted motion picture Loose Change. The exact file name was "911 — Loose Change 2nd Edition DVDRip (ConCen) XviD.avi." On the Mega Sites there were 97 other URL links pointing to the same infringing copy of Loose Change. In addition, the MD5 hash for the copy of Loose Change stored in DOTCOM's Megaupload.com account matched the file name and unique MD5 hash of infringing copies of Loose Change available on several third-party linking sites, one of which redirected to Megaupload.com.

*Inferences:* Mr Dotcom knew Mega hosted infringing content. He personally handled and stored infringing files hosted by Mega. His lack of concern about the infringing status of files within his knowledge mirrored his appreciation that the business involved attracting, distributing and hosting copyright infringing content.

*Mr Dotcom was aware that users, their files, the traffic flowing to their content and revenue derived from it, could be readily ascertained using Mega databases and other analytic tools available to the conspiracy.*

[348] The applicant alleges that examples of this knowledge include the following:

- (1) Mr Dotcom asked Mr Ortmann for the number of subscriptions purchased as a result of TH's activities. Mr Ortmann indicated this information could be quickly ascertained.<sup>92</sup>
- (2) Mr Ortmann was able to ascertain the daily link deletions performed by Warner Brothers in 2009 (2,500) and by a "cursory check" verified that "it's legit takedowns of content that they own appearing in public forums."<sup>93</sup>
- (3) Mr Dotcom expected that Mr van der Kolk and Mr Ortmann could "make a list of all links that were reported from Mexico, Brazil, and other non first world countries in the last 4 weeks and undelete all of them."<sup>94</sup>

Paragraph [31e]:

On or about June 29, 2010, after receiving a copy of the criminal search warrant, Ortmann sent an email entitled "Re: Search Warrant — Urgent" to DOTCOM and three representatives of Carpathia in the Eastern District of Virginia. In the email, Ortmann stated, "The user/payment credentials supplied in the warrant identify seven Mega user accounts", and further that "The 39 supplied MD5 hashes identify mostly very popular files that have been uploaded by over 2000 different users so far." [...].

[349] The applicant alleges that Mr Dotcom was aware of the techniques for identifying and filtering or blocking particular files. He acknowledges this in discussing the elimination of child pornography files but did direct similar measures to be applied to files that were known to infringe copyright.

Paragraph [31f]:418

---

<sup>92</sup> SROC 2 para [108d] (ROC bundle p 161).

<sup>93</sup> ROC 6 para [31d] (ROC bundle pp 22-23).

<sup>94</sup> SROC 2 para [133c 5] (ROC bundle pp 210-211).



E-mails between conspirators demonstrate that the Mega Conspiracy has eliminated known child pornography and other illicit content, including terrorist propaganda videos, by searching the system for identical MD5 hash values and deleting files with matching hash values. Members of the Mega Conspiracy have failed to implement a similar program to actually delete or terminate access to copyright-infringing content.

i. On or about April 8, 2007, DOTCOM sent an e-mail to PayPal, in which he stated that Megaupload.com was working toward "preventing pedophilic materials from being distributed through our service[.]" DOTCOM outlined their "key procedures", which included the following:

1. Keyword-based upload alerting. We maintain a list of patterns/words commonly used in relevant file names and descriptions. Whenever a new file is uploaded whose file name or description matches, the file is forwarded to our content auditing team for further inspection.

2. Recursive tracking of uploaders and files. When our team of content auditors receives a notification of an upload related to child exploitation either through (1), or from a 3rd party source, they verify the file's nature, then cross-match related uploads by IP, by the file's hash fingerprint, and by the supplied uploader credentials (user ID, e-mail addresses). This procedure is effective, because the same uploader often uploads more than one file, and the same file is typically uploaded more than once by different, unrelated persons. The process is applied repeatedly, leading to a step-by-step compromise of most file portfolios containing pedophilic material. Existing fingerprints are stored permanently and will immediately trigger an alarm if they match a new upload. The Mega Conspiracy failed to implement any similar procedures for copyright-infringing works.

ii. On or about August 14, 2007, DOTCOM and Van der Kolk received an e-mail, in which the author stated, "Apparently, there are questionable (possibly bestiality) videos on your site. Can you please have some over there remove the following videos which are shown on this screen shot?" Van der Kolk responded to the email, copying DOTCOM and Ortmann, as follows: "I cleaned up most bestiality."

iii. On or about August 14, 2010, DOTCOM sent an e-mail to hosting company executives DS and JK, and to Ortmann. <sup>3</sup> In the email, DOTCOM addressed the Mega Conspiracy's treatment of "Content that is illegal per se, most notably pedophilia material."

DOTCOM stated, "A specialized team of auditors is continuously putting great efforts into the discovery and elimination this type of content by looking at upload sources (user accounts, IP addresses) of newly reported files, then identifying similar items uploaded from the same source, leading to further upload sources. This process is applied recursively and exhaustively[.]" DOTCOM further stated, "As a result, the frequency of notices coming from established monitoring bodies such as 'Telefono Arcobaleno' has decreased to near-zero as it is now well known in the criminal scene that abusing Megaupload for storing their appalling material would pose great risks to them."

*Inference:* Mr Dotcom was aware that copyright infringing files could be identified and deleted but instead ran the business to preserve access to such material.

***Prime Facie Evidence that Mathias Ortmann and Bram van der Kolk were members of the copyright conspiracy.***

[350] In the applicant's evidence it is alleged that Mr Ortmann and Mr van der Kolk are the most visible members of the copyright conspiracy. They say there are two reasons for this.

- (1) Mr Ortmann and Mr van der Kolk were senior officers of the Mega business and both occupied technical roles. They accordingly knew of, and implemented, the major decisions about the operation of the sites. They controlled the engine room of the sites.
- (2) They are also conspicuous because a large number of messages passing between them have been discovered and added to the ROC.

*The two men communicated in ways that showed they knew they were participants in an unlawful business whose profitability depended on large flows of traffic to copyright infringing material.*

[351] The applicant alleges that this is already set out in detail above.

*They were involved in manipulating viewing times to maximise purchase of subscriptions. In doing so, they were consciously exploiting users' appetite for commercial, copyright movies.*

[352] Paragraph [104d]:

On or about September 14, 2008, via Skype, ORTMANN told VAN DER KOLK, "imagine people being interrupted shortly before a movie ends," and "the inclination to pay will be higher than on MU." VAN DER KOLK responded, "pretty good point," and "this can be the new way of making revenue for Hollywood one day again :)"

Paragraph [104j]:

On or about September 28, 2008, via Skype, VAN DER KOLK asked ORTMANN, "Don't you think copyright holders will now get extra pissed?" ORTMANN responded, "they wouldn't know," because "they probably don't watch their own stuff for 60+ minutes :)"

Paragraph [104n]:

On or about November 21, 2008, via Skype, VAN DER KOLK and ORTMANN discussed the ideal time limitations to maximize the number of users who decide to pay for premium membership. VAN DER KOLK said, “we have to reach that critical point to cash in,” and “yes, but with MV people watch 90-120 minutes.” ORTMANN responded, “limitis beyond 3 hours – no conversion, 2 hours – some conversion, 90 minutes – more conversion, 70 minutes - major conversion,” and “there is a huge difference between 90 and 70 minutes there.” VAN DER KOLK then said, “lets see how many % clicks on the buy now button from the MV premium limitation message,” and “(this is very good btw, google analytics).” ORTMANN added, “yes, seems so”.

*Inference:* Messrs van der Kolk, Ortmann and Dotcom conspired to maximise revenue from traffic to copyright infringing commercial movies. At the same time they consciously injured the interests of copyright owners.

*The rewards scheme*

[353] The applicant alleges that this has been outlined extensively above and in paragraph [82] ROC. They say that dialogue throughout the ROC and SROCs places Mr Ortmann and Mr van der Kolk at the heart of the rewards scheme from its 2006 inception until its cessation in mid-2011.<sup>95</sup>

[354] Mr Ortman and Mr van der Kolk both dealt with batches of payments to repeat infringers and corresponded directly with some of them.<sup>96</sup>

[355] Paragraph [106j] is an illustration:

On or about January 25, 2008, via Skype, VAN DER KOLK and ORTMANN discussed a particular repeat infringer and unindicted conspirator (herein referred to as “JH”). VAN DER KOLK said, “his 500 and 1500 USD redemptions were disqualified” and “he has 6 \$100 redemptions pending.” ORTMANN said, “he probably has 100% fraudulent files in his account.” VAN DER KOLK responded, “most likely,” “that’s the big flaw in the rewards program” — “we are making profit of more than 90% infringing files,” “so either we should just lower the points a bit and pay everybody, or stop paying rewards.” VAN DER KOLK then said, “I asume with this rewards payment Kim wants to be very generous?” ORTMANN responded, “yes, but only for those users that brought premium sales :)”

<sup>95</sup> See, on the rewards scheme generally ROC para [25] (ROC bundle pp 16-19); on Ortmann’s and van der Kolk’s interaction with repeat infringers generally SROC 2 para [106] (ROC bundle pp 151-157).

<sup>96</sup> See for example the respondents’ correspondence with known and repeat infringer “TE” at SROC 2 para [110]. (ROC bundle pp 164-171).

[356] They discussed the portfolios of rewards claimants and the basis on which they would be paid or disqualified.

Paragraph [46f]:

On or about August 24, 2007, VAN DER KOLK sent an e-mail to ORTMANN, entitled "Reward payments." In the e-mail, VAN DER KOLK wrote, "Hereby the rewards batch payment file. Total costs: \$12,800 USD. Lot's of 1500 dollar redemptions from Vietnamese uploaders again..." VAN DER KOLK also wrote, "I checked every file / video portfolio; however let me know if it's too much, then I'll check who else we can disqualify for whatever reason :)" [...].

[357] They also studied the value of the infringers' content to Mega and the traffic and the relationship between rewards payments and growth of the business. For example, paragraph [106v]:

On or about November 8, 2009, via Skype, VAN DER KOLK and ORTMANN discussed a rewards payment of \$175,600. VAN DER KOLK said, "it's still very fine in relation to our costs / income / profit if you think about it," because "these users are making it happen." ORTMANN asked VAN DER KOLK about a particular repeat infringer and unindicted conspirator, referred to as LR in Paragraph 53 of the Record of the Case, "is that a big contributor," and VAN DER KOLK responded, "more than 70M video views." ORTMANN replied, "not bad VAN DER KOLK offered "but we can skip him if you want :)" and ORTMANN replied, "nono :)" "70M video views are worth up to 150K."

[358] *Inferences*: Mr Ortmann and Mr van der Kolk ran the rewards scheme in ways that prejudiced the rights of copyright owners. The evidence disclosed that they were paying users to upload infringing content and make it available on the internet, they did not delete files, block access, or terminate the users' accounts.

*Both men misled copyright owners about Mega's response to takedown notifications*

[359] Paragraphs [82] and [83] explain, how in early-mid 2008, Sony Pictures Entertainment Inc. and NBC Universal received confirmation from Mr van der Kolk that: "Simply copy and paste one or multiple links into the text area [of the Abuse Tool] and the videos and/or files will be removed from our system immediately." Both Sony and NBC relied on these misrepresentations and continued to submit takedown requests instead of pursuing additional action against Mega<sup>97</sup>.

---

<sup>97</sup> Paras [82c] and [83b] (ROC bundle p 112-113).

[360] In another email to a copyright holder, Mr van der Kolk maintained that complainants need only “Simply copy and paste one or multiple links into the text area [of the Abuse Tool] and the videos and/or files will be removed from our system immediately.”<sup>98</sup>

[361] The applicant alleges that a similar misrepresentation was made by Mr Ortmann to Irdeto, a company who submitted takedown requests on behalf of copyright holders, in May 2008. Mr Ortmann maintained in an email to Irdeto “We are taking great care in expeditiously deleting any material reported to us through DMCA takedown notices.”<sup>99</sup> Irdeto relied on this misrepresentation and continued to submit takedown requests instead of pursuing additional action against Mega.<sup>100</sup>

[362] The applicant alleges that the well-documented reality was that files were not removed – only individual links to those files were ever removed.<sup>101</sup> Mr Ortmann and Mr van der Kolk made these misrepresentations to retain access to underlying files and the traffic and revenue they attracted.

*Inference:* Mr van der Kolk and Mr Ortman deliberately misled copyright owners about Mega’s response to notified copyright infringements.

[363] The applicant alleges that in a similar vein, Mr Ortmann deceived Paypal over the response to certain specific infringements, and deceived the USTR by falsely describing the operation of the rewards scheme and the general policy towards copyright infringement.

*Inference:* If allowing continued access to infringing files was believed to be lawful, it would not have been necessary to practise these deceptions. The fact that Mr Ortmann pretended files were indeed being deleted shows that he knew this was what Mega should have been doing. By criticising the rewards schemes of Mega’s competitors, he showed an awareness that Mega’s own conduct had been unlawful while its rewards programme remained in existence.

---

<sup>98</sup> Paras [96a] (ROC bundle pp 118-119).

<sup>99</sup> Para [34f] and [94a] (ROC bundle p 30, 118).

<sup>100</sup> Para [94c] (ROC bundle p 118).

<sup>101</sup> See above para [244] ff.

*They each received large numbers of takedown notices but failed to ensure that files were deleted or all links to infringing content were disabled*

[364] Mr van der Kolk was responsible for, and received the lion's share of, takedown notices.

Paragraph [22k]:

I am an employee of Megaupload Limited ("Megaupload"), which operates a virtual locker service at <megaupload.com>. I am responsible for taking down content in response to Digital Millennium Copyright Act (DMCA) takedown notices which are sent to Megaupload. As such, I am familiar with and have personal knowledge regarding its practices for receiving and acting on takedown notices, including those sent to the email address legal@megaupload.com.

[365] Mr Ortmann also handled takedown notices.

Paragraph [128b]:

During the 2010 calendar year, PayPal representatives sent ORTMANN over 115 notices referencing more than 2,000 URL links to copyright infringing materials on the Mega Sites.

[366] However, it is alleged that both men routinely failed to ensure the underlying files the notices related to were disabled.

Paragraph [128d]:

A preliminary review of the databases shows that despite ORTMANN's claims that the uploaded files had been deleted, the Mega Conspiracy merely disabled the specific URL links identified in the notices. And despite ORTMANN's claims that approximately 220 registered users had been blocked, as of January 19, 2012, only approximately 18 of those users were blocked from using the Mega Sites on that date.

[367] The applicant alleges that Mr van der Kolk's dealing with takedown notice is detailed extensively through the "repeat infringers" sections of the ROC<sup>102</sup>. A clear example of the effect of failing to remove underlying files is shown at paragraph [49a]:

According to a preliminary review of the databases, on September 7, 2009, a particular repeat infringer, premium user, and unindicted conspirator (herein referred to as "BM"), created a URL link to an infringing copy of the

---

<sup>102</sup> See paras [46] and [106] (ROC bundle pp 67-70, 151-157).

copyrighted computer software The Sims 2. The exact file name was "(PC GAME ITA) The Sims 2 CD1.iso." BM's description of the file included the Internet website baixemuito.com, a third-party linking site that featured copyright-infringing computer software and television programs. That infringing software was downloaded more than 7,300 times through BM's link prior to December 17, 2009, when the Mega Conspiracy processed a takedown request for the file. The takedown request was processed manually by defendant VAN DER KOLK, who disabled access only to the link and not to the infringing content. The infringing file remained accessible on the Mega Sites because other links pointed to the same file. On or about December 21, 2009, four days after VAN DER KOLK processed the takedown request, BM created a second URL link to the same infringing file, again listing baixemuito.com in the description. The infringing software was downloaded more than 27,000 times through BM's second link prior to March 16, 2010, when a representative of the copyright owner submitted another takedown request through the Abuse Tool. The following day, March 17, 2010, the takedown request was processed manually by defendant VAN DER KOLK, who disabled access only to the second link and not to the infringing content. The infringing file remained accessible on the Mega Sites through other active links. On March 17, 2010, BM created a third link to the same infringing file, again listing baixemuito.com in the description. The infringing software was downloaded more than 80,000 times through BM's third link prior to September 1, 2010, when VAN DER KOLK manually processed another takedown request for the file. VAN DER KOLK disabled access only to the third link, and the infringing file remained accessible on the Mega Sites through other active links. On September 1, 2010, BM created a fourth link to the same infringing file, again listing baixemuito.com in the description. VAN DER KOLK manually processed a takedown request for the file on an unknown date, disabling access only to the fourth link and not to the infringing content. The infringing file remained accessible on the Mega Sites through other active links. On July 1, 2011, BM created a fifth link to the same infringing file, again listing baixemuito.com in the description. This fifth link was still active as of January 19, 2012. In total, the Mega Conspiracy received over 1,500 takedown requests for URL links created by BM through his uploads of copyright-infringing content to the Mega Sites. Despite having received these takedown requests, the Mega Conspiracy never terminated BM and never purposefully and completely blocked access to the infringing content.

*Inference:* Mr Ortmann and Mr van der Kolk deliberately did not use the database to remove copyright infringing content, or to identify users who persistently made available copyrighted material the subject of takedown notices.

*They had control over the deletion of links and the suspension of users*

[368] The applicant alleges that the responsibility for deleting files and links often, if not always, fell to Mr Ortmann and Mr van der Kolk. For example, in 2010 a PayPal representative sent Mr Ortmann over 115 takedown requests relating to over

2000 URL links. Mr Ortmann’s response is outlined in the extract below, at paragraph [128c]:

ORTMANN responded to these copyright-infringement notices by assuring PayPal that the infringing file had been removed or deleted, and — for approximately 220 of the approximately 330 registered users — that the user had been blocked from using the Mega Sites (for the remaining users, ORTMANN either failed to mention the user entirely, or he indicated that the user had been warned). For example, on or about September 17, 2011, ORTMANN wrote the following two-sentence response: “All infringing uploads have been deleted and their uploader blocked. Thank you for forwarding this DMCA notice!”

[369] Mr Ortmann and Mr van der Kolk had control over suspending repeat infringers. Paragraph [106n] is an example:

On or about April 15, 2008, via Skype, VAN DER KOLK sent ORTMANN a portion of an e-mail sent by a representative of Warner Brothers Entertainment Inc. to the Mega Conspiracy at dmca@megavideo.com. The portion of the e-mail stated:

The following user [USERNAME REDACTED] appears to have circumvented Megavideo. When you look at his profile he shows that he has uploaded only 7 videos to Megavideo. However, this is not accurate. This user is circumventing Megavideo by linking to infringing videos directly and not searchable via Megavideo. Since these television episodes below prove that user [USERNAME REDACTED] has hidden and marked his videos as private, content owners such as Warner Bros. are unable to search and find all infringing content. I would like to request that his account be suspended. Below is an example of infringing content found from the linking site for user [USERNAME REDACTED].

The full e-mail also included multiple URL links to copyright-infringing materials, including the copyrighted television programs Smallville and Terminator: Sarah Connor Chronicles. Attached to the e-mail were two photographs, the first depicting the user’s profile on Megavideo.com, and the second depicting a copyright-infringing video of Smallville uploaded by the user. VAN DER KOLK commented via Skype to ORTMANN, “the copyright holders are also getting smarter, with screenshots and everything :)” ORTMANN responded, “wow :)” As of January 20, 2012, [USERNAME REDACTED]’s account was active.

[370] The applicant alleges that Mr Ortmann and Mr van der Kolk also consistently reinstated infringers’ accounts who were seen as valuable sources of content. For example, this passage concerning repeat infringer “TE”. Paragraph [110g]:



Accounts belonging to TE were repeatedly suspended for violating Megaupload's Terms of Service regarding copyright infringement. Despite these suspensions, TE's accounts were reactivated by members of the Mega Conspiracy. For example, on or about September 9, 2007, VAN DER KOLK e-mailed TE and stated, "we're not paying out any rewards to users that upload copyright infringing material." On or about September 18, 2007, VAN DER KOLK informed TE by e-mail that his account was suspended again on September 17, 2007, because Megarotic's rewards desk "identified a number of uploads that may infringe on the intellectual property rights of third parties." On or about October 6, 2007, however, DOTCOM forwarded ORTMANN an e-mail from TE indicating that TE's account had been reinstated.

[371] This portion of the ROC goes on to detail how Mr Ortmann and Mr van der Kolk unblocked TE numerous times, despite flagrant copyright infringement. One reason for this is the value of Mr van der Kolk and Mr Ortmann saw in TE's as a prolific uploader of popular infringing content, at paragraph [110ii]:

On or about June 24, 2008, via Skype, VAN DER KOLK sent ORTMANN an e-mail from TE, in which TE alerted the Mega Conspiracy that he had more than 100 million video views. VAN DER KOLK commented, "what a guy :)" and ORTMANN, "wow:)"

[372] These shortcomings should not be misread as an inability to suspend users for violations – Mr Ortmann and van der Kolk several times used suspension to deal with users committing fraud against Mega.<sup>103</sup> Rather, the applicant's evidence shows Mr Ortmann and Mr van der Kolk strategically omitted to suspend uploaders so as to preserve content and revenue.

*Inference:* Van der Kolk and Ortmann turned a blind eye to copyright infringement on the Mega sites and encouraged the activities of known repeat infringers.

*Because of their responsibility for the software programming, both would have been aware that the most popular infringing content was copied onto Cogent servers for faster mass distribution*

[373] Paragraph [102f]:

As described in Paragraph 72 of the Record of the Case, software written by the Mega Conspiracy reproduced the most popular files onto faster Mega

---

<sup>103</sup> See, for example, para [114d]. MW's account was suspended for fraud against Mega. Also, TE's account was eventually finally blocked when he attempted to remove his content from the Mega sites to use on his own site. The conspirators blocked TE's access to his content and continued to make it available on the Mega sites: see paras [110uu] and [110vv] (ROC bundle pp 177-179, 171).

controlled servers owned by Cogent Communications. The software executed every 60 seconds on an infinite loop, checking whether the Cogent servers had enough free space to host additional popular files. If there was free space available, the software would download and reproduce the popular file from the Mega-controlled server where it was originally stored onto the faster Cogent server; the file also remained on the original server, resulting in multiple copies. The software measured popularity based on how much throughput, or bandwidth, was consumed by the file at that time. The software also removed files from the Cogent servers when the software determined that those files were not being distributed as frequently.

*Inference:* It is reasonable to infer that in their position as technology officers, Mr Ortmann and Mr van der Kolk would have been privy to the distribution function of the Cogent system, which clearly furthered distribution of popular infringing content.

They studied the nature of traffic flowing to Mega sites and understood that Mega relied on traffic to infringing content via third party linking sites.

[374] As previously described<sup>104</sup>, the respondents relied heavily on third party linking sites to access content hosted by Mega.

[375] Mr Ortmann and Mr van der Kolk studied the nature of traffic flowing to the Mega sites through these linking sites. Analytics accessed by the pair show the content these third party sites were linking was infringing.

Paragraph [331]:

On or about September 17, 2011, Van der kolk sent an e-mail to Ortmann, attaching a Google Analytics report on referrals to Megaupload.com from the linking site Taringa.net. The single page report indicates that, between August 17, 2010, and September 16, 2011, Taringa.net provided more than 72 million referrals to Megaupload.com, with the top 10 links including copyrighted software and music titles. The page indicates, for example, that the linking site produced 164,214 visits to Megaupload.com for a download of the copyrighted CD/DVD burning software package Nero Suite 10. This software program had a suggested retail price of \$99.

[376] The applicant's evidence suggests that such analytics were accessed by the conspiracy from at least 2008.<sup>105</sup> This information detailed, amongst other things, the sources of traffic to the Mega sites.

<sup>104</sup> See, for example, para [213].

<sup>105</sup> SROC 1 para [74e] (ROC bundle pp 105-106).

Mr Nomm describes how he and Ortmann discussed blocking third party linking sites for transgressions of various kinds, but “ORTMANN never mentioned blocking third-party linking sites for copyright-infringement to Nomm<sup>106</sup>.”

*Inferences:* Mr Ortmann and Mr van der Kolk knew that Mega relied heavily on traffic to infringing content. Traffic analysis confirmed the site was running according to the private front end/back end piracy model which they had intended. Mr Nomm confirms that the conspirators periodically discussed the role of third party linking sites in enabling traffic to infringing content on their sites.

*They knew from other evidence that users were accessing the sites to view and download infringing content.*

[377] The applicant alleges that Mr Ortmann and Mr van der Kolk were informed by copyright holders that infringing content was being accessed on the Mega sites.

Paragraph [106n]:

On or about April 15, 2008, via Skype, VAN DER KOLK sent ORTMANN a portion of an e-mail sent by a representative of Warner Brothers Entertainment Inc. to the Mega Conspiracy at dmca@megavideo.com. The portion of the e-mail stated:

The following user [USERNAME REDACTED] appears to have circumvented Megavideo. When you look at his profile he shows that he has uploaded only 7 videos to Megavideo. However, this is not accurate. This user is circumventing Megavideo by linking to infringing videos directly and not searchable via Megavideo. Since these television episodes below prove that user [USERNAME REDACTED] has hidden and marked his videos as private, content owners such as Warner Bros. are unable to search and find all infringing content. I would like to request that his account be suspended. Below is an example of infringing content found from the linking site for user [USERNAME REDACTED].

The full e-mail also included multiple URL links to copyright-infringing materials, including the copyrighted television programs Smallville and Terminator: Sarah Connor Chronicles. Attached to the e-mail were two photographs, the first depicting the user’s profile on Megavideo.com, and the second depicting a copyright-infringing video of Smallville uploaded by the user. VAN DER KOLK commented via Skype to ORTMANN, “the copyright holders are also getting smarter, with screenshots and everything:”

---

<sup>106</sup> SROC 6 para [170jj] (ROC bundle p 314).

ORTMANN responded, “wow:)” As of January 20, 2012, [USERNAME REDACTED]’s account was active.

Mr Ortmann and Mr van der Kolk are pointed directly to evidence of a user uploading infringing content for other users to access. The infringing user’s account remained active.

[378] Mr Nomm confirms that Mr Ortmann and Mr van der Kolk were aware of cases in which individual users were clearly accessing infringing content<sup>107</sup>.

*Inference:* Mr Ortmann and Mr van der Kolk knew users were accessing infringing files but did nothing to prevent this when particular cases came to their attention.

*They knew that Mega hosted a huge volume of infringing content*

[379] The volume of infringing content on the Mega sites is discussed frequently throughout the applicant’s evidence.

Paragraph [107f]:

On or about October 7, 2007, via Skype, VAN DER KOLK said to ORTMANN, “Maybe we should automatically delete videos on Megavideo that are longer than 30 minutes and have more than XXX views or something because I still see so much piracy that is being embedded.” VAN DER KOLK then asked, “What kind of videos are legit and longer than 30 minutes and views more than XXX times...” ORTMANN responded, “what we can indeed do is put them into ‘temporarily not available’ state and priority-audit them” and “anything that’s legit will then be unblocked permanently, the rest will go to deleted.” VAN DER KOLK responded, “yeah, but 99.999% will be deleted then.” Based on a preliminary review of the Mega databases and source code, as of January 19, 2012, it does not appear that the Mega Conspiracy implemented a copyright screening feature for videos longer than 30 minutes based on the number of views.

Paragraph [103aa]:

On or about September 5, 2008, via Skype, ORTMANN told a third-party individual at an Internet hosting provider, “Switzerland features some interesting locations for server hosting” because “deep inside some mountain, the data will survive nearly all natural and man-made disasters.” The third-party individual responded, “yea - i dont think Megaupload needs to be up after a world ending nuclear war.” And ORTMANN replied, “it

---

<sup>107</sup> SROC 6 para [170m] (ROC bundle p 310).

[Megaupload.com] could serve as a pretty complete archive of the world's intellectual property for a coming generation.”

[380] Mr Nomm confirms that advertisers made that advertisers made many complaints about the prevalence of copyright infringing materials on Mega sites and these were forwarded to Mr van der Kolk<sup>108</sup>.

*Inference:* Ortmann and van der Kolk knew Mega hosted a very large volume of infringing material and were intent on exploiting the traffic that this attracted.

*They were privy to Mr Dotcom's decision to ignore "non first world" complaints*

[381] Mr Dotcom's initiative to ignore takedown notices from non-first world countries is detailed in the ROC at paragraphs [38] and [133]. Messrs Ortmann and van der Kolk are complicit in the infringement that followed Mr Dotcom's direction. At paragraph [133c 4] Mr Ortmann acknowledges they are ignoring "legitimate" takedown requests in an act of "calculated risk":

Later that day, ORTMANN told BENCKO, "the takedown notices were legitimate for sure," "however, calculated risk could work here".

[382] Paragraph [76b] shows Mr van der Kolk acting on Mr Dotcom's advice to undelete infringing links:

With respect to Paragraphs 38(j) and 38(k) of the Record of the Case, the emails sent by DOTCOM on April 23 and 24, 2009, relate to the same course of events. Also on April 23, 2009, VAN DER KOLK forwarded to ORTMANN the APCM's February 4, 2009 e-mail, writing, "another candidate for undeletion." Minutes later, VAN DER KOLK forwarded to ORTMANN the APCM's April 23, 2009 e-mail, writing, "also needs to be undeleted." Based on these e-mails, it appears that access to the URL links identified by APCM had been disabled (although the underlying copyright infringing materials remained accessible through other URL links pointing to the same materials), and that DOTCOM instructed VAN DER KOLK and ORTMANN to "undelete" the URL links, thus making them available to the general public. As of January 19, 2012, approximately 4,600 of these 7,000 URL links to copyright-infringing materials were still active and available on the Mega Sites (roughly 2,400 URL links were disabled as a result of later copyright takedown notices; however, the copyright-infringing content remained accessible to members of the public).

---

<sup>108</sup> SROC 6 para [170aa] (ROC bundle p 313).

*Inference:* Messrs van der Kolk, Ortmann and Dotcom conspired to maintain access to copyright infringing files in circumstances where they thought there was limited risk of legal action.

*Ineffectual auditing*

[383] The applicant alleges Mr van der Kolk was responsible for an ineffectual auditing process that was designed to allow copyright infringing materials to remain on Mega sites and was aware of the limitations of the limited auditing that did take place.

Paragraph [74b] shows Mr van der Kolk had responsibility in auditing of content on the Mega sites:

On or about September 25, 2007, VAN DER KOLK sent an e-mail entitled "RE: Auditing" to an unindicted conspirator and employee of the Mega Sites. Attached to the e-mail was a text file "Auditor Guidelines," which contained the following instructions to employees responsible for auditing files on the Mega Sites:

Megarotic Video: Videos that have to be set to private:  
 - Long length high quality videos that are obvious ---  
 - Video with known logos / website URL's in it of copyright holders

Megavideo:  
 - Mark sexy / soft erotic (non nude) videos as private  
 - Delete soft erotic with nudity  
 - Delete pornographic / extreme nudity (visible organs /penetration / etc.) and block the user  
 - Delete hateful I violent content (obvious racism / real killing / torture, etc.)

Auditing for Megavideo is rather simple, just make sure that the above described stuff will be deleted and the rest of the videos can be approved.

Videos that were set to "private" were not publicly displayed on the front pages of the Mega Sites, but users still had the ability to distribute these URL links in the same manner as non-private links, for example, on third party linking sites.

[384] Mr van der Kolk's auditing policy avoided detection of copyrighted material by direct searching. By marking content "private" it will not show on Mega's front

page<sup>109</sup>, nor will the uploader be publically identifiable. “The rest of the videos” – which clearly includes copyright violating videos – can be approved. Mr Nomm confirms that Mr van der Kolk supervised an auditing process that was deliberately ineffective. It was “not a serious effort and was more about appearances than effectively addressing infringement<sup>110</sup>.”

[385] Mr Ortmann was aware of the broad mesh of Mega’s auditing system.

Paragraph [103rr]:

And ORTMANN added, “the important thing is that nobody must know that we have auditors letting this stuff through.” VAN DER KOLK responded, “yes that’s very true also.” ORTMANN replied, “if we had no auditors – full DMCA protection, but with tolerant auditors, that would go away.” And VAN DER KOLK replied, “yes true”.

[386] Paragraph [106d] further emphasises Messrs Ortmann and van der Kolk were aware of the shortcomings of the auditing process:

On or about April 10, 2007, via Skype, VAN DER KOLK said to ORTMANN, “we should definitely pay all of the uploaders in the beginning,” and, “they will make us big.” ORTMANN then asked, “are new uploads currently audited for copyright violation?” VAN DER KOLK responded, “not yet, I am sending specs to Andrus [NOMM] shortly.”

[387] Mr Nomm demonstrates that Mr Ortmann deliberately ignored filtering options that would have improved auditing by identifying files with the characteristics of infringement. Mr Ortmann did not want to employ techniques that “would prove that they had the ability to easily filter content on Megavideo.com<sup>111</sup>.” Mr Ortmann also knew that the “video querying tool” could be used to identify high definition content likely to include significant numbers of infringing files<sup>112</sup>.

*Inferences:* Messrs Ortmann and van der Kolk ran an auditing process which they knew would not exclude copyright infringing content. They knew that this practice would expose Mega to legal sanctions unless it remained secret. Ortmann wanted to preserve the “dumb pipe” cover story.

---

<sup>109</sup> Para [74b] (ROC bundle p 104).

<sup>110</sup> SROC 6 Para [170u] (ROC bundle p 312).

<sup>111</sup> SROC 6 para [170v] (ROC bundle p 312).

<sup>112</sup> SROC 6 para [170ww] (ROC bundle p 312).

*They were conscious of maintaining a sanitised, “innocent front end” to the sites, while the lucrative traffic to infringing content took place through the “private” back end via direct links and embedded players.*

[388] The applicant alleges that Mr Ortmann and Mr van der Kolk marked videos longer than 10 minutes as “private”.

Paragraph [102c]:

When a user uploaded a video file to Megavideo.com, software written by the Mega Conspiracy added an entry to the internal database, which include the following information about the video (not a comprehensive list): unique MD5 hash; video name; video description; upload date; the number of times the video had been viewed; the identification number of the user who uploaded the video; the 8-character download identifier for use with the URL link associated with the video; whether the URL link had been the subject of a copyright-infringement takedown request; and whether the video was “private.” Software written by ORTMANN and VAN DER KOLK marked all videos longer than 10 minutes as “private.” As discussed in Paragraph 74(b) of the Record of the Case, “private” videos were not publicly displayed on the front pages of the Megavideo website, but users still had the ability to distribute these URL links in the same manner as non private links (for example, on third-party linking sites).

[389] Mr Ortmann and Mr van der Kolk went to lengths to limit direct searchability on the Mega sites.

Paragraph [33a]:

Megaupload.com does not provide a search function, and although Megavideo.com does provide a search function, any search for a full length copyrighted video will not produce any relevant results. Instead, the Mega Conspiracy business model relies on thousands of third-party “linking” sites, which contain user-generated postings of links created by Megaupload.com (as well as URL links created by other Mega Sites, such as Megavideo.com and Megaporn.com). While the Mega Conspiracy may not operate these third-party sites, for years the Mega Conspiracy offered the program described above in the section entitled Uploader Rewards Program, which provided a direct financial incentive for premium users to post URL links on linking sites.

[390] The search function was provided by third party sites, so as to obscure the wealth of infringing content housed on the Mega sites.

Paragraph [107d]:



On or about August 30, 2007, via Skype, ORTMANN asked VAN DER KOLK, “how clean are the existing videos on MRV now, what do you think?” The acronym “MRV” appears to refer to the streaming section of Megarotic.com. VAN DER KOLK responded, “it’s pretty clean from the perspective of child porn / disgusting stuff,” “but still lot’s of copyright infringements.” He added, “if we want to clean things up we have to agree on what has to go and what not,” “otherwise I can delete 90% of the content :-)” Then VAN DER KOLK said, “right okay,” “so videos longer than 10 minutes on MRV should be set to private or something...” and ORTMANN responded, “yes,” but “direct linking / embedding is fine.” VAN DER KOLK added, “embedded players are not so harmful.” ORTMANN commented, “searchability is dangerous and will kill us,” and VAN DER KOLK replied, “yeah.”

[391] Conversion of video files to “Flash Video” format was crucial to wide distribution of content through embedded players.

Paragraph [102d]

When a user uploaded a video file to Megavideo.com, software written by the Mega Conspiracy converted the video file — including those tagged as “private” — to a particular video format known as Flash Video or “FLV.” A flash-version of the video allowed quicker and broader distribution of files by the Mega Conspiracy because Flash videos could be streamed through most Internet browsers with a high level of compression at fast download speeds.

[392] Messrs van der Kolk and Ortmann were aware that conversion facilitated distribution of infringing content through embedded players.

Paragraph [103q] explains:

On or about November 14, 2007, via Skype, DOTCOM said to ORTMANN, in German, “Will you eventually solve the conversion problem. The complaints don’t stop. What do you think you can do?” ORTMANN responded “We have a long queue of DVD-rips” “and some DRM protected, that cannot be converted”. DOTCOM replied “Then we need more conversion servers, please order”. The acronym “DRM” refers to “Digital Rights Management” and is commonly understood to mean copyright-protection based in either software, such as encryption, or somewhat less commonly, hardware. During that time period, the Mega Conspiracy was converting user-uploaded videos, including copyrighted videos, into a particular video format known as Flash Video or “FLV”, which facilitated the video’s distribution.

*Inference:* Messrs Ortmann and van der Kolk were responsible for design features that they knew would disguise the presence of infringing files on Mega sites. They also took steps to facilitate the viewing of infringing content via third party sites.

*They were involved in the acquisition of YouTube videos and the manipulation of the Megaupload “Top 100” list.*

[393] The applicant alleges that Mr Dotcom’s intention to mass copy YouTube videos is detailed above and Messrs Ortmann and van der Kolk played an active and conscious role in this scheme.

Paragraph [38a]:

On or about April 10, 2006, Van der Kolk sent an e-mail to Ortmann asking, "Do we have a server available to continue downloading of the Youtube's vids? ... Kim just mentioned again that this has really priority." In addition, Van der Kolk wrote, "Hope [Youtube.com] is not implementing a fraud detection system now... \* praying \*". Van der Kolk also wrote: "Well we only have 30% of their videos yet.. In my opinion it's nice to have everything so we can descide and brainstorm later how we're going to benefit from it."

Mr Nomm confirms Mr van der Kolk’s involvement in acquiring and exploiting the YouTube videos<sup>113</sup>.

*Inferences:* In an effort to disguise Mega’s reliance on infringing files, Messrs Ortmann and van der Kolk manipulated the content of the Megaupload “Top 100”. They also unlawfully acquired YouTube video clips. They used them to create the false impression that Mega was primarily a site that hosted “user-generated content.”

*They were personally aware of infringing files on the sites and they obtained links to infringing files and circulating them.*

[394] The applicant alleges that:

- (1) Messrs Ortmann and van der Kolk knew how to locate infringing files via the database;
- (2) They had knowledge Mega hosted infringing content;
- (3) They were indifferent to the infringement which their use of the files represented; and

---

<sup>113</sup> SROC6 para [170t] (ROC bundle p 311).

- (4) This state of mind is consistent with their knowing participation in a business that aimed to exploit the distribution of copyright infringing materials

[395] The applicant says Mr van der Kolk provided a set of obviously infringing links to an unindicted conspirator.

Paragraph [129]:

On or about February 17, 2007, VAN DER KOLK sent an e-mail to an unindicted conspirator, entitled “links for my little megaupload addict! :-)” The e-mail listed links that had been uploaded to Megaupload, including the Megaupload URL link, corresponding file name, and file size. VAN DER KOLK organized the links according to various categories.

1. The “Justin timberlake movies” category listed 33 links, 1 of which was marked “Deleted=5.” According to a preliminary review of the Mega databases, “Deleted=5” indicated that the link had not been accessed within a specified period of time and had expired. Justin Timberlake is an American actor, performer, and singer-songwriter.
2. The “Porn” category listed 100 links, 4 of which were marked “Deleted=5,” and 1 of which was marked “Deleted=1 .” According to a preliminary review of the Mega databases, “Deleted=1” indicated that the link had been deleted due to an abuse report.
3. The “weight loss” category listed 12 links, 1 of which was marked “Deleted=5,” and 1 of which was marked “Deleted=99.” According to a preliminary review of the Mega databases, “Deleted=99” indicated that the link had been deleted by the user.
4. The “yoga” category listed 100 links, 12 of which were marked “Deleted=5.”
5. The “oprah” category listed 100 links, 3 of which were marked “Deleted=5.” Oprah Winfrey is an American talk show host, actress, producer, and philanthropist.
6. The “mad tv” category listed 100 links, 5 of which were marked “Deleted=5.” Mad TV is a copyrighted television series.
7. The “harvey birdman” category listed 3 links, 1 of which was marked “Deleted=5.” Harvey Birdman, Attorney at Law, is a copyrighted television series.
8. The “arrested development” category listed 100 links, 11 of which were marked “Deleted=5.” Arrested Development is a copyrighted television series.

[396] Paragraph [79] shows that Mr van der Kolk also had an active account and content portfolio from which other users downloaded infringing content:

VAN DER KOLK maintained a number of active accounts on the Mega Sites. One of his Megaupload.com accounts contained infringing copies of copyrighted works uploaded by VAN DER KOLK, including a variety of motion pictures and television programs.

These copyright-infringing works included books from the graphic novel series Inuyasha and Shigurui; episodes from the television programs Earth: The Power of the Planet, Ugly Betty, Venus Versus Virus, and The Last Days of Lehman Brothers; and the motion pictures Bruno, Taken, Open Season 3, Legion, and L'Italien. On the Mega Sites there were more than 2,400 other URL links pointing to the same infringing copy of L'Italien; more than 800 URL links pointing to the same infringing copy of Bruno; and more than 150 URL links pointing to the same infringing copy of Ugly Betty. The URL links created by VAN DER KOLK for the infringing copy of the motion picture Bruno received approximately 97 downloads or views by users of the Mega Sites.

[397] Mr Van der Kolk also acted as a conduit to infringing content for the other respondents, as shown by:

Paragraph [39c]:

On or about August 15, 2007, Bencko sent Van der Kolk an email message indicating: "the sopranos is in French :((( fuck,. can u pis find me some again?" "The Sopranos" is a copyrighted television series that previously aired on the premium channel Home Box Office.

Paragraph [39d]:

On or about October 4, 2007, Bencko sent Van der Kolk an email message entitled "pis" requesting: "can u pis get me some links to the series called 'Seinfeld' from MU?" "Seinfeld" is a copyrighted television series that remains in syndication.

Paragraph [39e]:

On or about October 18, 2007, Bencko sent an e-mail to Van der Kolk indicating that "sorry to bother but if you would have a second to find me some links for the 'Grand Archives' band id be very happy." On or about the same day, Van der Kolk responded to Bencko with an e-mail that contained a Megaupload.com link to a Grand Archives music album with the statement "That's all we have. Cheers mate!"

[398] Mr Ortmann was personally familiar with the infringing content available on the Mega sites.

Paragraph [103o]:

On or about September 30, 2007, via Skype, ECHTERNACH asked ORTMANN, in German, “send me a mega link to an xp installation cd ;)” ORTMANN responded, “need to screen through it, just a second.” Approximately 1 day later, via Skype, ORTMANN sent ECHTERNACH a URL link, which had been uploaded by a Mega user, to the copyright protected computer operating system “Windows XP USB Edition” on Megaupload.com. Approximately three hours later, ECHTERNACH responded, “USB Edition?!” ORTMANN then sent ECHTERNACH another URL link uploaded by a separate mega user to the non-USB edition of “Windows XP” on Megaupload.com. Windows XP is a copyrighted software program owned by Microsoft Corporation. The “USB Edition” refers to a version of Windows XP available on a USB drive.

[399] Earlier that year Mr Ortmann distributed another link to a “Windows XP”, this time to Mr Dotcom.

Paragraph [103c]:

On or about February 7, 2007, via Skype, ORTMANN sent DOTCOM a URL link to the copyrighted computer software Microsoft Windows SP, which had been uploaded by a registered Megaupload user.

[400] At the requested of an unindicted person Mr Ortmann searched for obviously infringing content.

Paragraph [103i]:

On or about March 4, 2009, via Skype, VAN DER KOLK told ORTMANN, “I downloaded some bluray rips with Mega Manager over night, downloaded a whopping 50GB+ in about 14 hours :)” and ORTMANN responded, “damn:)” In this context, the phrase “bluray rips” appears to refer to infringing copies of copyrighted Blu-ray Discs.

*Inferences:* Ortmann and van der Kolk were aware of, and had personal access to, files handled by Mega that clearly infringed copyright. Despite this, they took no steps to remove such content. This was because they appreciated the conspiracy was aimed at exploiting access to infringing content.

*They downloaded “ripped” files*

[401] Paragraph [103ff]:

[402] On or about March 4, 2009, via Skype, VAN DER KOLK told ORTMANN, “I downloaded some bluray rips with Mega Manager over night, downloaded a whopping 50GB+ in about 14 hours :)” and ORTMANN responded, “damn:)” In this context, the phrase “bluray rips” appears to refer to infringing copies of copyrighted Blu-ray Discs.

**Prima Facie Evidence that Mr Batato was a member of the copyright conspiracy**

[403] The applicant alleges that Mr Batato and Mr Dotcom have known each other since at least 1992<sup>114</sup>. Mr Batato was employed in the Mega business towards the end of 2007, and became the Chief Marketing and Sales Officer for Megaupload Limited<sup>115</sup>. In 2010 he personally received more than \$400,000 from the Mega business<sup>116</sup>.

[404] The applicant’s evidence is that Mr Batato:

- (1) Knew that Mega hosted large volumes of copyright infringing material, particularly movies and television programmes, which were in high demand among users;
- (2) Knew that this content was disguised on Mega sites. Commercial content could not be directly searched because if that could happen, “it would basically mean that we can shut down Mega ;-)<sup>117</sup>”;
- (3) Knew that copyright material, such as movies, could be located on third party linking sites and viewed or downloaded by accessing a Mega URL. Users obtained access to infringing files in exactly this manner;
- (4) Personally accessed infringing content in this way;
- (5) Sold Megaclick advertising to sites he knew were “warez movies sites”. The advertisements for such sites were visible to users of Mega sites. In this way Mega directly profited from the copyright

---

<sup>114</sup> SROC 4 para [136a] (ROC bundle p 229).

<sup>115</sup> SROC 4 paras [136o] [22m] (ROC bundle pp 230, 12).

<sup>116</sup> ROC para [22m] (ROC bundle p 12).

<sup>117</sup> SROC 4 para [160b] (ROC bundle p 264).

infringements for which those “warez” sites were responsible, and thereby assisted in their copyright infringing activities<sup>118</sup>;

- (6) Knew that pirated anime content was highly popular but arranged advertising on Mega sites for a repeat infringer, paid by Mega, who specialised in links to anime content;
- (7) Knew Mega had a piracy reputation which made it hard to sell advertising to large, reputable businesses;
- (8) Knew there was a perception that Mega was associated with the linking site Kino.to. When this site was taken down in June 2011 and its operators arrested, a wave of alarm passed through the conspirators, including Mr Batato. Mr Ortmann observed to Mr Batato that Mega must distance itself from the kind of “organised crime” – Mr Batato’s phrase – that Kino.to had been conducting. The same month that Kino.to was taken down, Mega ended its rewards scheme; and
- (9) Received “on numerous instances... DMCA copyright infringement takedown notices from third-party companies”.<sup>119</sup>

[405] Advertising yielded the Mega business some US\$25m.<sup>120</sup> This revenue was dependent on traffic. On Megavideo, for example, “before any video can be viewed... the user must view an advertisement”.<sup>121</sup> This was referred to as “pre roll” advertising.<sup>122</sup>

[406] By managing this source of income, with knowledge that Mega concealed its hosting of copyright materials to benefit from traffic to that content, Mr Batato attached himself to the copyright conspiracy.

*Mr Batato knew that Mega hosted copyright infringing material and concealed the availability of that content*

---

<sup>118</sup> SROC 7 para [172].

<sup>119</sup> ROC para [22m] (ROC bundle p 12).

<sup>120</sup> ROC para [22h] (ROC bundle pp 9-10).

<sup>121</sup> ROC para [22h] ROC bundle pp 9-10).

<sup>122</sup> Para [39n] (ROC bundle pp 40-41).

Paragraph [33j]:

On or about January 28, 2010, in an e-mail entitled "activating old countries," a user of a Mega Conspiracy site asked Batato: "where can we see full movies?" Batato replied, "You need to go to our referrer sites. Such as www.thepiratecity.org or www.ovguide.com[.] There are the movie and series links. You cannot find them by searching on MV directly. That would cause us a lot of trouble ;-)"

*Inference:* Batato understood the innocent front end/ piracy principle on which the Mega sites operated. He was privy to the same kind of thinking which the Ortmann/van der Kolk skypes reveal.

Paragraph [172d]:

On or about July 27, 2010, by Skype, BATATO told NOMM that a particular ad seller "temporarily banned us because there were a lot of users coming from strange sites to us." NOMM responded, "look [at our] site names... look [at] our content... and then they should wonder why strange sites". NOMM then added, most of our content is stolen and uploade[d] by users." BATATO replied, "I know :D."

*Inference:* Mr Batato's exaggerated smile – ":D" – reveals that he fully agreed with the proposition that most of Mega's content was stolen. He knew himself that most of the traffic to Mega sites was via "strange sites" (i.e. linking sites) to that stolen content.

*Mr Batato knew that traffic – and therefore advertising revenue – depended on the availability of copyright infringing content, the presence of which was deliberately concealed on the Mega sites*

[407] Paragraph [160b]:

On or about October 24, 2011, via Skype, a third-part advertiser asked BATATO, referring to the Mega Sites, "what exactly do you require? do be able to target users by the content they watch basically, because a user that watches content about poker is better for us than the one who watches content about cooking an ostrage egg properly. :)" BATATO responded, "Ah okay. No that is not possible technically. That would mean that we could make the content searchable which would basically mean that we can shut down Mega ;-)" The advertiser then asked, "really? why? don't you want people to be able to find stuff?" BATATO responded, "Well you can find stuff, but you can't search for series, movies, etc". The advertiser asked, "but why don't you at least tag the videos by category or something?" BATATO responded, "The UGC is searchable. But you will not get enough traffic from those." In context, it appears that "UGC" refers to user-generated content, as opposed to copyright-infringing work that drove the traffic to the Mega Sites.



[408] Paragraph [160c]:

On or about December 14, 2011, via Skype, a third-party advertiser and "regular user" of Megavideo told BATATO that he has "been subscribed for over 3 years now" but "lately it is very slow to load tv shows, movies." The third-party noted that "back in the days" he "always used megavideo only" "because it was freaking fast." BATATO responded, "I will have that checked. Thx for letting me know."

*Inferences:* Mr Batato knew that Mega hosted copyright infringing files, a fact which had to be disguised. The extent of reliance on infringing content was such that, if the content Mega hosted was made directly searchable, it would quickly be shut down by legal action.

[409] The applicant alleges that advertising was at times directly associated with infringing content. Mr Batato and Mr Ortmann "asked NOMM to place advertisements directly within the videos, including, inevitably, videos that were copyright-infringing, that were displayed on the Mega Sites<sup>123</sup>." Given his responsibility for advertising revenue and his knowledge of the prevalence of infringing videos that Mega hosted, it is inevitable that Mr Batato knew the business profited in this direct manner from copyright infringement. This is confirmed by paragraph [170m]. All the respondents "were aware that they were making money directly from reproducing and distributing copyright-infringing content uploaded to the Mega Sites..." Moreover<sup>124</sup>:

NOMM was aware of millions of dollars being made through advertisements posted on the Mega Sites through Megaclick.com and he knew that these advertisements were displayed in connection with copyright-infringing content. NOMM understands that each visit to a page that was associated with copyright-infringing content and had advertising provided a direct monetary benefit to the Mega Conspiracy.

The applicant alleges that if Mr Nomm had this awareness, it is not conceivable that Mr Batato, who was "responsible for marketing and advertising sales through Megaclick.com", did not share the same knowledge.

*Mr Batato knew that third-party linking sites directed traffic to Mega*

---

<sup>123</sup> SROC 6 para [170bb] (ROC bundle p 313).

<sup>124</sup> SROC 6 para [170m] (ROC bundle p 310).

[410] The applicant alleges that its evidence shows that Mr Batato was aware that third-party linking sites acted as Mega's conduit to infringing content.

Paragraph [33h]:

On or about June 6, 2009, Batato sent an e-mail to an advertiser indicating, "Banners will be shown on the download pages of Megaupload. You will find some links here for example: <http://mulinks.com/news.php>".

Paragraph [33i]:

On or about November 30, 2009, Batato sent an e-mail to an advertiser stating: "Please go to mulinks.com and copy paste One of those URLs to your browser. You will then see where the banner appears."

Paragraph [39h]:

On or about October 13, 2008, Batato sent an e-mail to an advertiser, which included a screen capture of the Megaupload.com download page for the file "MyBlueBerryNights.part1.rar". The screen capture also contained an open browser window to the linking site www.mulinks.com. "My Blueberry Nights" is a copyrighted motion picture.

Paragraph [39i]:

On or about October 14, 2008, Batato sent an e-mail to an advertiser that contained two Megaupload.com links. One of the links directed to a file "DanInRealLife.part2.rar", which was a portion of an infringing copy of the copyrighted motion picture "Dan in Real Life."

*Inference:* Mr Batato knew these third party linking sites directed traffic to infringing content hosted by Mega. This offset the limited searchability of the Mega sites.

[411] Mr Nomm confirms that he and "each of the co-conspirators periodically discussed the fact that users often discovered copyright-infringing content stored on the Mega Sites through third-party linking sites<sup>125</sup>." The applicant therefore alleges Mr Batato was involved in such discussions.

*Mr Batato knew that users obtained copyright infringing materials on the Mega sites. This causes no apparent concern because it is the expected operation of the sites.*

Paragraph [39k]:

---

<sup>125</sup> SROC 6 para [170m].

On or about May 25, 2009, Batato sent an e-mail to Ortmann that contained customers' e-mails. One of the customer e-mails indicated: "We watched Taken successfully and then tried to watch the 'Alphabet Killer' a day later and got the message to upgrade if we wanted to continue watching." "Taken" and "The Alphabet Killer" are copyrighted motion pictures.

[412] Paragraph [39m]:

[413] On or about November 15, 2010, Mr Batato forwarded an e-mail to Ortmann entitled "member-issue" that was received by a Mega Conspiracy employee from a user. In the forward, Mr Batato wrote "Fanpost ;-)". The email from the user stated: "I paid yesturday however can't work it out!!!\ I have been trying to see Robin Hood, 3th season, chapter 10, and do not succeed. Please help me solve it — or cancel my payment!" "Robin Hood" is a copyrighted television series that was originally released by the British Broadcasting Corporation.

*Inference:* Mr Batato knew that copyright infringement was an intended feature of the operation of Mega sites.

*Mr Batato used linking sites to obtain or view copyright materials hosted by Mega*

[414] Paragraph [159]:

a. BATATO's Internet browsing history revealed that he had visited the following websites at the following dates and times:

i. On or about October 23, 2011, BATATO performed a Google search for the phrase "two and a half men," a copyrighted television series broadcast in the United States on CBS.

ii. On or about October 28, 2011, BATATO visited the third-party linking sites tvlinks.eu and watchseries.eu. On these third-party linking sites, BATATO visited webpages with the titles "Watch Online Two and a Half Men Season 9 Episode 5 —A Giant Cat Holding a Churro — Watch Series" and "Watch Two And A Half Men — Season 9 Episode 5: A Giant Cat Holding A Churro." That same day, BATATO visited on Megavideo.com a video file entitled "two.and.a.half.men.s09.e.05.hdtv.xvidfqm.FileW.arez.tv.avi." That link was uploaded on or about October 18, 2011, and remained active until on or about January 20, 2012.

iii. On or about January 10, 2012, BATATO performed a Google search for the phrase, "mu links," which appears to reference "Megaupload links." The website mulinks.net, which in this context refers to "Megaupload links," was a third-party linking site. That same day, BATATO visited mulinks.net and visited a video entitled "Virgin Territory 2007," which was hosted on Megaupload.com under the file name "Virgin.Territory.2007.DVDRip.XviD-ELia.part2.rar." That link was uploaded on or about January 30, 2008, had more than 200 downloads, and remained active until on or about January 20, 2012. "Virgin Territory" is a copyrighted motion picture.

*Inferences:* Mr Batato appreciated that third party sites provided ready access to infringing content hosted by Mega. Mega itself could not safely reveal the extent to which it hosted infringing files.

[415] Mr Batato is also known to have provided Mr Dotcom with a link to a copyright music file (Louis Armstrong – We have all the time in the world.mp3) which was located on Mega servers<sup>126</sup>.

*Mr Batato sold Megaclick advertising to sites he knew were “warez movies sites”*

[416] This is made clear from the exchanges set out in para [172]:

On or about March 11, 2010, by Skype, BATATO asked NOMM to approve an advertising campaign on Megaclick.com for JSC. NOMM responded that JSC was an “advertizer of full length movies and a “warez movies site.” BATATO immediately asked, “Yes, and?” NOMM replied, “ill ask Mathias [ORTMANN]... last time we talked deal was not to add obviously stolen content sites.” BATATO then asked, “What is the problem? Just want to understand”. NOMM responded, “According to Mathias [ORTMANN] its not good approve warez movies sites as its bad for MV”. BATATO then replied, But we have ireel also”. NOMM responded by asking BATATO to discuss the issue with ORTMANN. Despite this conversation, JSC was permitted to continue advertising on Megaclick.

On or about March 11, 2010, by Skype, NOMM and Ortmann discussed whether to allow “warez” sites to advertise directly on the Mega Sites. NOMM said, “for MV... I have ads... what links to warez site that has full length vidos”. ORTMANN responded, “actually, suicidal for MV” and then asked “Finn [BATATO] approved that?” NOMM replied, “sure he always does”.

On or about April 9, 2010, by Skype, BATATO told NOMM, “Be aware that advertising (cash” are as important as EVERYTHING else in the company.”

[417] The applicant alleges that:

- (1) By selling Megaclick privileges in this manner, Mr Batato made advertisements for “warez” sites visible to Mega users. Mega profited directly from the copyright infringing activities of those sites.
- (2) He did not care that Mega profited in this lawful manner, hence his responses: “Yes, and?” and “What is the problem? Just want to understand?”

---

<sup>126</sup> Para [38e] (ROC bundle p 34).

- (3) When mildly challenged by Mr Nomm he pointed to existing precedents for his practice, referring to the example of Ireel.
- (4) It is not clear whether he discussed the matter with Mr Ortmann, as Mr Nomm recommended. Either way, he allowed the JSC advertising to continue.
- (5) This was not an isolated incident, but rather a practice that Mr Batato followed. On another occasion when Mr Nomm and Mr Ortmann discussed “warez” sites advertising on Mega and linking to infringing videos, Mr Ortmann asked if Mr Batato approved this and Mr Nomm replied that “he always does.”
- (6) Mr Batato’s remark on 9 April 2010 shows that he was motivated by the desire to maximise advertising revenue.

*Inferences:* Mr Batato obtained income for Mega by allowing by assisting sites he knew were involved in copyright infringement to advertise on Mega sites.

- (7) By selling Megaclick privileges in this manner, Mr Batato made advertisements for “warez” sites visible to Mega users. Megaupload profited directly from the copyright infringing activities of those sites.
- (8) He did not care that Mega profited in this manner, hence his responses: “Yes, and?” and “What is the problem? Just want to understand?”
- (9) When mildly challenged by Mr Nomm he pointed to existing precedents for his practice, referring to the example of Ireel.
- (10) It is not clear whether he discussed the matter with Mr Ortmann, as Mr Nomm recommended. Either way, he allowed the JSC advertising to continue.
- (11) This was not an isolated incident, but rather a practice that Mr Batato followed. On another occasion when Mr Nomm and Mr Ortmann discussed “warez” sites advertising on Mega and linking to infringing

videos, Mr Ortmann asked if Mr Batato approved this and Mr Nomm replied that “he always does.”

- (12) Mr Batato’s remark on 9 April 2010 shows that he was motivated by the desire to maximise advertising revenue.

*Inferences:* Mr Batato obtained income for Mega by allowing sites he knew were involved in copyright infringement to advertise on Mega sites.

*Mr Batato and anime*

[418] In 2008 and 2009, Mr Batato sold advertising to repeat infringer DR, whose advertising campaigns were listed in Mr Batato’s correspondence as “2008-11-05 WatchMyAnime” and “2009-09-04 Animebayocom<sup>127</sup>.” As these names suggest, the subject matter of these advertising campaigns was anime, a genre of video material protected by copyright. In earlier correspondence with Mr van der Kolk, DR had asked whether he had been suspended for uploading anime and was specifically warned against uploading adult material to Megavideo instead of Megarotic<sup>128</sup>.

[419] The applicant alleges that it is reasonable to infer that a user, seeking to advertise anime, was doing so for the purpose of publicly distributing copyright material for some financial advantage – in DR’s case to obtain Mega uploader rewards. The circumstances enable an inference of knowledge that the advertising would facilitate DR’s infringement of copyright.

[420] An exchange between Mr Ortmann and Mr Batato in September 2008 also concerned anime. Mr Batato inquired about a site at <http://www.anime.net>. Mr Ortmann replied that this was “a pirate download-link site for animes. It’s not legal, but it is not forbidden for them to advertise with us.” The conversation then turned to the income that would be obtained from this advertising, with Mr Ortmann concluding “I feel better then<sup>129</sup>.” This should have reinforced an understanding that traffic to anime content was likely to be pirate in nature.

---

<sup>127</sup> SROC 2 para [121d] and [121h].

<sup>128</sup> SROC 2 para [121c].

<sup>129</sup> SROC 4 para [155c].

*Inference:* Mr Batato helped Mega obtain revenue from traffic to infringing content.

*Mr Batato and the takedown of the Kino.to website*

[421] On 13 June 2011, Mr Batato identified three elements that made the Kino.to operation “crazy”: it ran a hoster, it ran a referrer site and it paid people to upload content<sup>130</sup>. Mega had two of these elements: it hosted content and paid uploaders, but was not significantly searchable and did not directly associate itself with a linking site. By the end of the month, Mega had abandoned the payment of rewards as well.

[422] On 6 July 2011, Mr Batato emailed Mr Ortmann, forwarding emails from an advertising entity which wanted to discontinue its advertising with Mega because of concerns related to the Kino.to takedown. Mega was either perceived as operating in a similar manner, or was associated with Kino through its referral service. On 8 August 2011, Mr Batato described Kino.to as “super fraud” and “organised crime” Mr Ortmann agreed and added “we have to separate ourselves from that.” The cessation of rewards payments at this time is more than coincidental and indicates knowledge that this practice was unlawful.

*Inference:* Mr Batato knew of the rewards programme and appreciated that Mega had been unlawfully paying users to upload infringing files.

*Mega’s piracy reputation made it hard for Mr Batato to earn advertising revenue*

[423] The applicant alleges Mr Batato knew that Mega’s lifeblood was traffic to the infringing content it hosted. This knowledge was reinforced by the reluctance of legitimate advertisers to have dealings with such a website business. The applicant’s evidence is that advertisers and others regularly shared these concerns, which are illustrated by the following examples:

Paragraph [39n]:

On or about February 25, 2011, Batato sent an e-mail to Nomm and Van der Kolk regarding problems with getting "pre-roll" advertising for Megavideo.com because of a "copy right issue." His e-mail contains messages between employees of Megaelick.com and a third-party advertising service. In

---

<sup>130</sup> SROC 2 para [121c].

an early message, the Megacllick.com employee informs Batato that the third-party advertising service considers it illegal to monetize infringing content through advertising immediately prior to viewing the content.

Paragraph [160e i]:

On or about May 6, 2011, via Skype, NOMM said to BATATO, "we need some more quality customers . . . no[t] this shady home sitting hackers :)" BATATO responded, "The problem is that those are the clients whose ads work with our traffic :-( No brand advertiser has interest in us. It is quite frustrating for the sales department. But we will focus more on gambling/gaming now." NOMM responded, "well we have not the best market."

Paragraph [160e ii]:

On or about June 16, 2011, via Skype, an unindicted conspirator said to BATATO in German, "we are too 'illegal' for German brands" which "deters our current ads." During a follow-up Skype conversation between the two on or about July 5, 2011, BATATO said in German, "we are on a blacklist on some of the networks, meaning that we are not booked because the advertisers are afraid."

Paragraph [155b]:

[...]On or about August 3, 2011, via Skype, BATATO said to ORTMANN in German, "It's not easy to sell ourselves to the elite advertisements with all those buzz words like license piracy, and all the other things we have to listen to. But we continuously improve. :)"

Paragraph [148e i]

On or about March 26, 2011, via Skype, DOTCOM asked BATATO in German, "How are things going with the new sales team?" BATATO answered, "So so. The US-boys are being difficult because the Media agencies pick on the Content License Topics. Will get together with the ad tech folks and see how we can approach the market better."

Paragraph [148e ii]:

On or about July 28, 2011, via Skype, BATATO said to DOTCO in German, "Essentially we are seeing an increase of concerns in regards to Copyright/DMCA."

*Inference:* Mr Batato appreciated the extent of Mega's reliance on traffic to infringing content.

*Mr Batato and Mega's cover story*



[424] Despite his alleged knowledge that Mega deliberately exploited the uploading and distribution of infringing content, Mr Batato propagated the cover story that Mega was DMCA compliant and its Abuse Tool removed infringing content.

Paragraph [160e iv]:

On or about December 6, 2011, via Skype, an unindicted conspirator chatted with BATATO in German and referred to Megaupload as "illegal." BATATO responded, "We are not illegal . . . We are a technology provider, nothing else than Youtube or Google (please don't refer to us as illegal, I don't like it because it's not correct). The reason for the campaign is to show that the world as well." The conspirator responded, "Finn, I don't communicate that externally. But when you search google for movies/stream or download, you get to us. I would love to call a brand and not always get hit over the head with that ... that is why I always say cloud, online storage . . . not file sharer."

Paragraph [160e iii]:

On or about October 14, 2011, via Skype, a third-party advertiser told BATATO, "You know I always fight to have big campaigns run on megaupload and megavideo[.] our client tell me not legal[.] blah blah[.] I tell their[,] come on it is the new century[.] people will watch stuff etc in all cases wheter you want or not so at least share the success of those websites." BATATO responded, "True." He later added, "Also we are following DMCA. Even more strict than Youtube."

Paragraph [160d]:

On or about April 26, 2011, via Skype, BATATO told an unindicted conspirator, "All the major studios have access to our servers in order to delete files themselves." [...].

*Inference:* Mr Batato appreciated that Mega relied on copyright infringement but tried to disguise this by asserting that it complied with DMCA obligations.

*Mega and Hong Kong traffic*

[425] Mega did not provide service in Hong Kong, where megaupload.com and megavideo.com were registered and where several of the respondents lived. The alleged reason was that they wished to avoid legal problems, especially relating to copyright infringement, where the companies were based.

[426] Mr Batato alluded to the motive for this in an email in 2010.

Paragraph [391]:

On or about February 1, 2010, Batato sent an e-mail to an unindicted co-conspirator with the subject "[tradeit] — Campaign stats" stating: "We can't deliver [Hong Kong] traffic because the company is based in [Hong Kong] and we don't want to experience any trouble with license holders etc. Remember, I told you about that topic ;-)".

[427] A later Skype message confirms the concern with legal actions originating in the state where Megavideo and Megaupload were registered<sup>131</sup>:

The U.S. Attorney's Office for the Eastern District of Virginia expects a representative of the FBI to testify to the following facts:

a. Members of the Mega Conspiracy blocked access to the Mega Sites from Internet Protocol addresses from Hong Kong. Internet Protocol addresses on a "white list," however, including those from Hong Kong, were permitted to access the Mega Sites.

b. On or about March 28, 2011, via Skype, a third-party told BATATO, "finn finn" "i need more traffic in HK!" BATATO responded, "Sweety, there is no traffic in HK." The third-party replied, "but you are from there," BATATO explained, "That's why

we don't serve traffic there," The third-party asked, "really?" BATATO responded, "Yes." The third-party replied, "i'm not sure I get it," And BATATO responded, "We are listed in HK. We just don't want to take any legal risk"

*Inference:* Mr Batato appreciated the business's operations were unlawful and exposed it to the risk of legal action. To reduce the risk of actions being filed in the Hong Kong jurisdiction, service was not provided to Hong Kong Internet protocol addresses, except in special "white list" cases.

---

<sup>131</sup> SROC 5 para [165].

*Payment of Rewards for Infringing Content*

[428] The applicant alleges that it is a reasonable inference that Mr Batato, because of his position in the business, knew that that it paid rewards for popular content. This was a basic feature of the Mega sites.

[429] They also say that Mr Batato plainly understood that Mega relied for its traffic upon people accessing copyright content. The traffic to user-generated content was negligible or insufficient. Copyright content was accessed through linking sites, a procedure with which he was clearly familiar. The content hosted by Mega could not be directly searched on the site because that “would basically mean that we can shut down Mega ;-).”

[430] They further say it is a further reasonable inference that Mr Batato understood the relationship between the payment of rewards on one hand and, on the other, the publication on linking sites of URLs pointing to large volumes of copyright material on Mega sites. Otherwise there was no incentive to upload and distribute access to infringing content on such a scale. He was responsible for Mega’s advertising revenue, which he knew depended on high traffic volumes of traffic to infringing content. The rewards scheme obviously played a significant part in attracting that content.

[431] The applicant alleges that when Mr Batato sold advertising to repeat infringer DR, he would have readily understood the incentive for running such advertising campaigns. DR was trying to attract viewers to anime content he had uploaded. It would be hard to account for his behaviour without suspecting the incentive of rewards.

[432] Mr Batato’s knowledge that the rewards scheme operated unlawfully can also be inferred from his response to the demise of the Kino.to sites. He viewed their operation as “organized crime” and thought they were “... crazy to run a hoster AND a referrer site AND pay people to upload stuff.” It was clearly dangerous for a site that posed as a cyberlocker to pay uploaders, and the rewards scheme was quickly dropped after these exchanges.

[433] The applicant therefore alleges that Mr Batato therefore “participated in” the company with knowledge of its unlawful operations in general, and also with particular knowledge that its rewards scheme attracted the infringing content on which his advertising revenue depended.

## **Preliminary Matters to be Heard**

### ***Stay Applications***

[434] Three applications for a stay of proceedings have been filed by the respondents:

1. A stay application dated 14 July 2015 had two aspects. The first related to an alleged financial “starve out” policy of the applicant to deprive the respondents from being able to engage and pay for overseas legal and technical experts to provide evidence at the eligibility hearing. The second aspect alleged a conflict of interest of Crown Law acting as counsel for the applicant in these proceedings and representing the Crown;
2. A stay application amended on 21 August 2015 relating to alleged unlawful/unreasonable conduct by the applicant;
3. A stay application dated 16 September 2015 alleging abuse of process by the applicant.

### ***Eligibility Hearing***

[435] The hearing to determine whether a person is eligible for extradition takes place in the District Court. The Court must be satisfied, that the appropriate supporting documentation has been produced, that the offence is an extradition offence in relation to the extradition country and that there is sufficient evidence relating to the offending that would justify the person’s trial if the conduct constituting the offence had occurred in New Zealand. Any applicable mandatory restrictions or discretionary restrictions on surrender will also be considered by the Court.

[436] If the Court determines that the person is eligible for surrender, the matter is referred to the Minister of Justice for a final decision. The person or requesting country may exercise appellate rights to the High Court on any questions of law arising from the District Court decision.

## PART B

### Stay applications

[437] The first issue to be addressed is: *Does the District Court have jurisdiction to hear stay applications during an eligibility hearing?*

[438] For the applicant it is submitted that if this Court has jurisdiction it is a narrow jurisdiction which excludes the consideration of collateral matters, such as those being submitted by the respondents. In addition, the applicant submits that, if applicable, there are adequate remedies elsewhere through other forums and these are currently being pursued.

[439] There is New Zealand case law on point. In *Police v D*<sup>132</sup> the Court of Appeal found that the committal Court had exceeded its jurisdiction by allowing inquiry into:

... allegations concerning the gaining of an advantage in a child care dispute, entrapment, police partiality and misconduct, and witness misconduct.

(as summarised in the headnote.)

[440] It went on to say<sup>133</sup>:

Having carefully considered these allegations and the context in which they arise, and having the benefit of the lengthy further judgment of the District Court Judge [staying the proceeding] in which he sets out fully his views of the evidence, we do not see how these matters bear upon the evidence of the elements of the offences charged. They may be entirely reprehensible and may call for action elsewhere but the present focus must be on the function of the committal proceeding<sup>134</sup>.

---

<sup>132</sup> *P v D* [1993] 2 NZLR 526 (CA).

<sup>133</sup> At p 532.

<sup>134</sup> At p 532.

...

P is alleged to have taken advantage of his position to extort money from W. That does not bear upon the alleged offence. The police are said to have acted improperly in dealing with a staff member of the Family Court and with the matter of bail ... They do not bear upon the offence. Reference has been made also to certain unsatisfactory aspects of the apparent non-availability of Telecom records but that too is beside the point. Questions surrounding admissibility of evidence including the legality of the recording of the conversation and entrapment are matters for the trial Judge. Accordingly we consider that to venture into the allegations of conduct beyond that bearing upon the matter at hand was to go beyond the jurisdiction of the Court in conducting a preliminary hearing.

[441] In *Bujak v Republic of Poland*<sup>135</sup> the Court of Appeal applied *Police v D* to an eligibility hearing. In that case they said:

[10] ... However, counsel for Mr Bujak, Mr Illingworth QC, contends that there remains a discretion on the part of the District Court to decline to order surrender on the basis that the delays that have been occasioned in the pursuit of Mr Bujak's extradition are of such significance that they amount to an abuse of process and the District Court's inherent power to prevent an abuse of its own processes applies in the context of extradition proceedings.

...

[33] We conclude that a District Court exercising jurisdiction under s 22 has the same power to avoid an abuse of its process as it has when conducting a committal hearing. This Court's decision in *Police v D* applies.

...

[38] Mr Lange [for the Republic of Poland] argued that the scope of any abuse of process jurisdiction was very limited. He pointed to the limited function of a District Court in the context of a s 24 hearing, namely to decide eligibility for surrender. The Court must, in terms of s 24(2)(d), satisfy itself that the evidence against the person for whom extradition is sought would justify the person's trial if the conduct constituting the offence had happened in New Zealand ...

[39] Mr Lange said that this Court had made it clear in *Police v D* that it would only be in exceptional cases that a court conducting committal proceedings would be entitled to stay the committal proceedings to avoid an abuse of process ...

...

[64] ... we uphold the submission of Mr Lange, that the role of a District Court conducting a s 24 hearing in the context of the Poland/NZ

---

<sup>135</sup> *Bujak v Republic of Poland* [2008] 2 NZLR 604 (CA)

Treaty is limited: the Court simply determines eligibility for surrender, and does not go on to consider whether there are circumstances justifying a refusal to surrender someone who is otherwise eligible for surrender.

[65] That means that the very limited abuse of process jurisdiction described in *Police v D* applies in this case. Mr Illingworth argued for a broader jurisdiction, citing the comments of Lord Griffiths in *R v Horseferry Road Magistrates Court, ex parte Bennett* that the abuse of process jurisdiction of magistrates in the United Kingdom is confined to the fairness of the trial of the particular accused with whom they are dealing, covering issues such as delay or unfair manipulation of court procedures. We do not accept that that statement, made in the context of a serious abuse (the accused had been subjected to illegal rendition to the United Kingdom), represents the law in New Zealand: rather, we adopt the position outlined by this Court in *Police v D*.

[66] Applying *Police v D*, it would not be open to the District Court in the present case to stay the s 24 hearing because of delays which may affect the fairness of Mr Bujak's trial or his ability to conduct his defence. Those are matters for the trial court in Poland ...

[442] The effect of *Police v D* and *Bujak* is that an extradition court should ensure fairness at the hearing but should not look beyond the charges and the evidence before it to see if a prima facie case has been made out. It should venture no further. In a later case, *R v Antonievic*<sup>136</sup>, it was found that there had been "grave" misconduct by Police which involved the placing of false information upon the Court's records. This was found to be an abuse of the Court's process and undermined public confidence in the integrity of the criminal justice system.

[443] In the extradition case of *R (Government of the USA) v Bow Street Magistrates Court*<sup>137</sup>, the High Court of England and Wales held that:

[84] The judge should be alert to the possibility of allegations of abuse of process being made by way of delaying tactics. No steps should be taken to investigate an alleged abuse of process unless the judge is satisfied that there is reason to believe that an abuse may have taken place. Where an allegation of abuse of process is made, the first step must be to insist on the conduct alleged to constitute the abuse being identified with particularity. The judge must then consider whether the conduct, if established, is capable of amounting to an abuse of process. If it is, he must next consider whether there are reasonable grounds for believing that such conduct may have occurred. If there are, then the judge should not

<sup>136</sup> *R v Antonievic* [2013] 3 NZLR 806 (CA).

<sup>137</sup> *R (Government of the USA) v Bow Street Magistrates Court* [2006] EWHC 2256.

accede to the request for extradition unless he has satisfied himself that such abuse has not occurred ...

[444] The Canadian approach is similar. In *Cobb v United States of America*<sup>138</sup> the Canadian Supreme Court confirmed that its courts do have a general discretion to prevent abuses of process:

[37] Canadian courts have an inherent and residual discretion at common law to control their own process and prevent its abuse. The remedy fashioned by the courts in the case of an abuse of process, and the circumstances when recourse to it is appropriate were described by this Court in *R v Keyowski* [1988] 1 SCR 657 at pp 658-59:

The availability of a stay of proceedings to remedy an abuse of process was confirmed by this Court in *R v Jewitt* [1985] 2 SCR 128. On that occasion the Court stated that the test for abuse of process was that initially formulated by the Ontario Court of Appeal in *R v Young* (1984) 40 CR (3d) 289. A stay should be granted where “*compelling an accused to stand trial would violate those fundamental principles of justice which underlie the community’s sense of fair play or decency*”, or where the proceedings are “*oppressive or vexatious*” ([1985] 2 SCR [128] at pp 136-37). The Court in *Jewitt* also adopted “the caveat added by the Court in *Young* that this is a power which can be exercised only in the ‘clearest of cases’” (p 137).

[38] When a stay of proceedings is entered in a criminal case for abuse of process, “the prosecution is set aside, not on the merits but because it is tainted to such a degree that to allow it to proceed would tarnish the integrity of the court”: *R v Conway* [1989] 1 SCR 1659 at p 1667. The remedy is reserved for the clearest of cases and is always better dealt with by the court where the abuse occurs: *R v Jewitt* [1985] 2 SCR 128.

[445] In New Zealand our Supreme Court in *Siemer v Solicitor-General*<sup>139</sup>, said at para [114]:

The courts’ inherent powers include all, but only, such powers as are necessary to enable a court to act effectively and uphold the administration of justice within its jurisdiction. Their scope extends to preventing abuse of the courts’ processes and protecting the fair trial rights of an accused”.

[446] In *Dotcom v USA*<sup>140</sup> McGrath and Blanchard JJ on the issue of disclosure did address the District Court’s inherent power and said:

<sup>138</sup> *Cobb v United States of America* [2001] 1 SCR 5878.

<sup>139</sup> *Siemer v Solicitor-General* [2013] 3 NZLR 441 (SC).

<sup>140</sup> *Dotcom v USA* [2014] 1 NZLR 355 (SC).



[160] Whether or not the District Court has an inherent power to order disclosure either generally or in relation to specific material in the possession of a foreign state accordingly turns on whether it is necessary for the Court to have such power to act effectively to prevent abuse of the court's process and to protect the fairness of the extradition hearing.

[447] This was confirmed by William Young J, who cited *Siemer* and said:

[227] Whether there is an inherent power to require general disclosure turns on whether such a power is necessary to enable an extradition court to act effectively and fairly.

[448] Glazebrook J said at:

[309] ... It seems to me to be axiomatic that the District Court must have the inherent power to ensure that there is a fair hearing. Indeed, there is a statutory acknowledgment of that position in s 22(1)(a) of the Extradition Act, which gives the courts the same jurisdiction and powers as if the proceedings were a committal hearing. It is also reinforced by the Bill of Rights and common law requirements for natural justice.

[449] It can therefore be concluded that this Court does have jurisdiction to hear a stay application that is based upon an allegation of abuse of the Court's process.

[450] The second issue is: *What is the test to be adopted for a stay application?*

[451] In a decision dated 14 December 2015 *Wilson v R*<sup>141</sup> our Supreme Court has considered the issues relevant to a stay application. The majority in that Court found that:

- (1) The granting of a stay application for the purpose of maintaining the integrity of the judicial system is an "extreme remedy which will only be given in the clearest of cases: at [60].
- (2) A stay may be granted: (1) where state misconduct has prejudiced the fairness of a defendant's trial; or (2) where a trial would undermine public confidence in the courts (at [40]). In the second category, the purpose of the stay is to preserve the moral integrity of the courts and

---

<sup>141</sup> *Wilson v R* [2015] NZSC 189 (SC).

not to discipline state agencies (at [50]) citing *Fox v Attorney-General*.<sup>142</sup>

- (3) In deciding whether to stay a proceeding for abuse of process, the court must weigh the public interest in maintaining the integrity of the justice system against the public interest in the accused standing trial. This assessment will turn on the particular matter before the court (at [60]).
- (4) The matters listed in s 30(3) of the Evidence Act 2006, and whether Evidence Act remedies would be sufficient, may be relevant to this assessment (at [60]).
- (5) The Court considered the issue of causation: specifically the relevance of whether the matter would have come to trial “but for” the Police misconduct. The Supreme Court concluded that causation in this sense is a relevant, but not necessarily a decisive, consideration (at [78]-[80]).
- (6) The factors relevant to the granting of a stay application for abuse of process include: the maintenance of public confidence in the courts; the seriousness of the offending; the impact of the misconduct; the attitude of the agency in question; the urgency which motivated the conduct; and whether alternative remedies could be granted (at paras [91]-[92]).

[452] In *Wilson* the Supreme Court found that Police behaviour amounted to “serious misconduct”, it had undermined the integrity of the court system and threatened judicial independence.

[453] However the majority dismissed the application for a stay of proceedings as the conduct was not systemic or in bad faith, repetition was unlikely and exclusion of evidence was an appropriate remedy (at [93]).

[454] Adopting the approach of *Bow Street* and the guidance of our Supreme Court in *Siemer*, *USA v Dotcom* and *Wilson v R*, this eligibility Court needs to:

---

<sup>142</sup> *Fox v Attorney-General* [2002] 3 NZLR 62 (CA).

- (1) Decide whether the conduct alleged to constitute an abuse has been clearly identified;
- (2) If that is established, is the conduct complained of capable of amounting to an abuse of process?
- (3) If it is, are there reasonable grounds for finding that such conduct occurred?
- (4) If so, would that abuse prevent the Court from conducting a fair hearing?
- (5) Recognise that the granting of a stay is an extreme remedy given only in the clearest of cases when it is necessary to maintain the integrity of the judicial system.

[455] In step (b) above this eligibility Court needs to consider whether the conduct complained of “would violate those fundamental principles of justice which underlie the community’s sense of fair play or decency”: *R v Keyowski*<sup>143</sup>. The common law rights for natural justice and rights of the respondents under our New Zealand Bill of Rights Act 1990 must also be considered in conjunction with the need to prevent any abuse of this Court’s processes.

### **Stay Application 1: Funding restrictions**

#### ***Background Context***

[456] On 14 July 2015 the respondents filed an application to permanently stay the eligibility hearing on the grounds of abuse of process. The respondents claimed that their ability to conduct a proper defence to the extradition application had been prejudiced by restrictions on their funding for legal expenses due to the conduct of the applicant in obtaining restraining and forfeiture orders from the US District Court over specified assets of the respondents.

---

<sup>143</sup> *R v Keyowski* [1988] 1 SCR 657 at pp 658-659.

[457] The context to this first stay application can be traced back to January 2012 when Judge O’Grady, of the US District Court of the Eastern District of Virginia, issued restraining orders on 10 and 25 January 2012 over the respondents’ bank accounts and other assets located in Hong Kong and New Zealand. In respect of the New Zealand-located assets only two of the respondents, Mr Dotcom and Mr van der Kolk, had restrained assets in New Zealand. Messrs Dotcom, Ortmann and van der Kolk held bank accounts in Hong Kong, which were restrained by the Hong Kong Special Administrative Region Court of First Instance (Hong Kong Court) on 18 January 2012.

[458] Once the restraining orders over the NZ assets were obtained the applicant then requested in April 2012 the assistance of the NZ Commissioner of Police, as authorised by the Attorney-General, to apply for registration of these orders as foreign restraining orders in the NZ High Court pursuant to the provisions of the Mutual Assistance in Criminal Matters Act 1992 (MACMA) and the Criminal Proceeds (Recovery) Act 2009 (CPRA). The High Court registered the foreign restraining orders on 18 April 2012<sup>144</sup>. Only the High Court may release restrained funds to meet the respondents’ legal and living expenses in New Zealand.

[459] However, a US Supreme Court decision<sup>145</sup> effectively prevents any of the respondents’ restrained funds being used to meet the legal fees of any US lawyers engaged by the respondents, given a causal nexus between the alleged offending of the respondents and the money in their US bank accounts.

[460] Mr Dotcom’s US counsel, in reliance on subsequent US case law exceptions, filed motions to release restrained funds to meet legal fees and to preserve data on the computer servers unplugged by the US authorities in 2012. These motions were unsuccessful. No funds would be released by US courts to pay the respondents’ legal expenses for proceedings conducted in the US and overseas, including the eligibility proceedings in New Zealand. The respondents’ attempts to enter into negotiations with the US Department of Justice for the release of funds were also unsuccessful.

---

<sup>144</sup> The restraining orders, issued by His Honour O’Grady J of the US District Court for the Eastern District of Virginia in January 2012, were registered in New Zealand subject to specified conditions imposed by Her Honour Potter J on 18 April 2012 in *The Commissioner of Police v Dotcom & ors* [2012] NZHC 634.

<sup>145</sup> *Caplin & Drysdale, Chartered v United States* 491 U.S. 617 (1989).

[461] In the interim the Hong Kong Court ordered on 29 July 2013 the release of restrained funds to Mr Ortmann and Mr van der Kolk to meet their reasonable legal costs in New Zealand, and in Mr Ortmann's case to also meet his reasonable living costs in New Zealand.

[462] Twelve months after the Hong Kong Court's release order the applicant sought civil forfeiture of the respondents' restrained assets in an *in rem* action brought in the US District Court on 29 July 2014. This prompted the respondents, through their US counsel, to file claims on 28 August 2014 declaring an interest in specified restrained assets, followed by a motion to dismiss or stay the forfeiture application on 10 October 2014. In response the applicant filed a motion to strike out the respondents' claims on 17 November 2014 in reliance on the doctrine of fugitive disentitlement. This motion to strike out was opposed by the respondents.

[463] Judge O'Grady ultimately granted the motion to strike and dismissed the respondents' claims on 27 February 2015. His Honour applied the doctrine of fugitive disentitlement against the respondents. The application of this doctrine, which is codified in US law<sup>146</sup>, prevents persons who are avoiding criminal prosecution in the United States from being able to seek the assistance of United States' courts to pursue a claim in a civil forfeiture action. The doctrine or principle of fugitive disentitlement is not recognised in New Zealand<sup>147</sup>.

[464] Under US law, in defending the extradition application in New Zealand the respondents were deemed to be "fugitives" in the US and were therefore disallowed under the codified doctrine from contesting the forfeiture application in the US District Court.

[465] On 12 March 2015 the NZ High Court granted an interim variation<sup>148</sup> to the New Zealand registered restraining orders enabling the High Court to release to Mr Dotcom and Mr van der Kolk some restrained funds up to \$700,000 under the supervision of Mr Galbraith QC in order to meet their legal expenses for various litigation proceedings including the forthcoming eligibility hearing.

---

<sup>146</sup> Title 28, United States Code, Section 2466.

<sup>147</sup> *Erceg v Erceg* (2014) 22 PRNZ 245 at [22] (His Honour Venning J) and *Dotcom v The Deputy Solicitor-General* [2015] NZHC 1197 at [79] (Her Honour Ellis J).

<sup>148</sup> *Commissioner of Police v Dotcom & van der Kolk* [2015] NZHC 458 (Her Honour Courtney J).

[466] On 27 March 2015, having already disentitled the respondents and dismissed their claims to an interest in the restrained property, Judge O’Grady of the US District Court issued on a default judgment basis civil forfeiture orders against the respondents’ restrained domestic and foreign assets. Appeals were subsequently filed in April 2015 against the decisions to strike out the respondents’ claims and to order default judgments against them. These appeals have yet to be heard by the US courts at the date of this judgment.

[467] On 18 April 2015 the NZ High Court<sup>149</sup> released from restraint significant further funds to Mr Dotcom and Mr van der Kolk. But this did not resolve the respondents’ funding issues due to their involvement in other litigation proceedings overseas, including in the United States.

[468] After having obtained the US civil forfeiture orders, the applicant requested the Commissioner of Police, under MACMA, to seek registration of these foreign forfeiture orders in the NZ High Court. In opposing the registration application Mr Dotcom and Mr van der Kolk sought judicial review of the Deputy Solicitor-General’s (Criminal) written authorisation to the Commissioner of Police to apply for registration of the forfeiture orders in the High Court. Both respondents, who were the plaintiffs in that proceeding, also sought interim orders from the High Court preventing the Commissioner from progressing the registration application, pending the substantive review hearing. In response the Deputy Solicitor-General and the Commissioner of Police applied to strike out the judicial review proceeding. The Commissioner submitted that relief under s 143 CPRA was available to the two plaintiffs (Mr Dotcom and Mr van der Kolk) should the foreign forfeiture orders be successfully registered in New Zealand.

[469] In a judgment dated 3 June 2015<sup>150</sup> Her Honour Ellis J refused to strike out the judicial review proceeding and granted interim relief orders to the respondents. Her Honour held that once a foreign forfeiture order was registered in New Zealand s 143 CPRA did not confer on the subject of that order a right to apply for relief from the operation of that order. The consequences of registration of the forfeiture orders

---

<sup>149</sup> *Commissioner of Police v Dotcom & van der Kolk* [2015] NZHC 761 (Her Honour Courtney J), reasons given in judgment [2015] NZHC 820.

<sup>150</sup> *Dotcom & van der Kolk v The Deputy Solicitor-General* [2015] NZHC 1197 (Her Honour Ellis J).

on the plaintiffs (the two respondents) were noted in Her Honour's judgment as follows:

[98] Accordingly my present view is that s 143 does not afford the plaintiffs with a right to apply for relief once the registration order is made. If that proves to be correct, registration would not only have the effect of more or less irreversibly vesting their assets in the Crown but it would potentially deprive them of the means to defend the pending extradition proceedings and to pursue their appeal from the fugitive disentitlement decision in the United States. As Courtney J's recent judgment indicates, it seems that they will only have the necessary funds to pay their legal advisers if they have [sic] continue to have recourse to a portion of their presently restrained/frozen assets.

[99] Accordingly, it seems to me that the consequences of registration for the plaintiffs in this case may well be more permanent and more serious than:

- (a) they were understood to be by Judge O'Grady;
- (b) they were submitted to be by Mr Boldt; and
- (c) they were (presumably) understood to be by the Deputy Solicitor-General (Criminal).

[470] Her Honour issued a declaration that the Commissioner of Police was to take no further action that was consequent upon the decision by the Deputy Solicitor-General (Criminal) to authorise him to apply to register the foreign forfeiture orders made by Judge O'Grady until further order of the High Court<sup>151</sup>.

[471] The US forfeiture orders were also unable to be registered in Hong Kong which, under their law<sup>152</sup>, requires the respondents' US appeals against those orders to be finally determined before the Hong Kong Court may consider the application for registration.

[472] Subsequent to Ellis J's judgment, on 24 June 2015 the applicant informed the respondents that any monies released by the High Court from restrained funds and paid to counsel or experts outside New Zealand would be forfeited to the United States and any person in receipt of restrained money would be prosecuted in a US criminal court. As a consequence the respondents sought clarification repeatedly

---

<sup>151</sup> At [135].

<sup>152</sup> Section 28 of the Mutual Legal Assistance in Criminal Matters Ordinance (Hong Kong).

from the applicant as to its position on the availability of funding for the respondents' defence in the eligibility proceeding.

[473] Meanwhile the Deputy Solicitor-General subsequently advised Mr Dotcom and Mr van der Kolk on 3 July 2015 that the Commissioner of Police's authority to apply for registration of the foreign forfeiture order was withdrawn. Although a reconsideration of the authorisation would occur after the eligibility hearing upon giving 10 working days' notice.

[474] On 3 September 2015 the US Department of Justice finally responded to the respondents' request for assurances in relation to funding of overseas legal costs for the forthcoming eligibility proceeding. Under cover letter of Crown Law dated 4 September 2015, the US Department of Justice advised the Deputy Solicitor-General that funds released by the NZ High Court to the respondents under the supervisory regime could only be utilised for living and legal expenses within New Zealand. The United States refused to provide an assurance to the respondents that it would not prosecute or seek a civil recovery from persons or entities located in the United States who were in receipt of restrained funds. Effectively, the NZ High Court variation order of 12 March 2015 would not be accommodated in respect of payments to persons or entities located in the United States for services rendered to the respondents.

[475] The Department of Justice's letter did not specifically refer to the restrained funds in Hong Kong. Mr Ortmann and Mr van der Kolk were concerned that the applicant would enforce its US forfeiture orders against funds released by the Hong Kong Court and paid to non-New Zealand based parties. Both respondents submit that aside from the assets frozen in Hong Kong they have no other financial resources available to fund their defence of the eligibility application.

[476] In the case of Mr Dotcom his access to beneficiary income from his family trust, the Trust Me Trust, and to NZ business income earned whilst on bail, which he relied on to pay his legal and living expenses, became subject to an interim freezing order on 25 November 2014 as a consequence of High Court proceedings brought by the Motion Picture Association of America and recording industry companies.



Consequently he says he was in financial straits by the end of November 2014 with no foreseeable income to fund the legal costs required to defend the eligibility application.

[477] At the eligibility hearing all the respondents contended that such funding for legal expenses was necessary in order to instruct US counsel, and to engage industry practice and technical experts in the US to provide evidence at the eligibility hearing, but the position adopted by the applicant meant they had been unable to do so. They argue an inability to mount a defence at the eligibility hearing without the benefit of this expert evidence from American witnesses will result in a breach of natural justice rights. Therefore an application for a permanent stay of proceeding is sought on the basis that the respondents will not be able to have a fair eligibility hearing in accordance with the principles of natural justice.

[478] Further the respondents contend that as a result of the applicant's position, unless the proposed overseas witnesses agree to assist them on a no-fee basis, they are unable to engage, brief or call any expert witness from outside New Zealand. Only Professor Lawrence Lessig, a professor of law at Harvard Law School, and Mr Ira Rothken, Mr Dotcom's American legal counsel, were prepared to provide their services on a no-charge basis to the first respondent, Mr Dotcom. In addition the respondents claim that the applicant's delay in reaching a decision on this funding issue, despite repeated requests over the period from the end of April 2015 to the beginning of September 2015 and in several High Court teleconferences during this period, caused the respondents a loss of valuable preparation time for the eligibility hearing.

[479] Prior to hearing the submissions on this stay application this Court issued a minute dated 2 October 2015 for the order of hearing with respect to all three (3) of the stay applications filed by the respondents. In relation to this 14 July 2015 stay application the minute stated:

- (a) The stay application (14 July 2015) as to the alleged financing "starve-out" policy of the applicant preventing the respondents from obtaining overseas legal and technical evidence – legal argument only as to whether such evidence is relevant at the eligibility hearing.

## **The Respondents' Submissions**

[480] The respondents submit that the applicant's refusal, to assure them that US recipients paid from restrained funds would not be the subject of court proceedings, has severely impacted upon their ability to instruct counsel and expert witnesses in the US to mount a defence to the eligibility proceeding. The respondents submit the following issues in respect of this stay application:

- (1) Inability to adequately understand and reply to the case against them;
- (2) Inability to advance legal arguments on matters of lack of candour, whether the alleged offences are extradition offences, and the interpretation and application of the United Nations Convention Against Transnational Organized Crime (TOC);
- (3) Inability to assess and respond to United States' affidavit evidence as to the legal position in the US;
- (4) Inability to advance technical arguments as to the operation of Mega;
- (5) Delay and distraction caused by the applicant;
- (6) Prejudice caused by the applicant;
- (7) Abuse of process by the applicant.

These issues are set out in greater detail in the following paragraphs:

### ***Respondents Adequately Understanding & Replying to the Case Against Them***

[481] The respondents submit that natural justice, at its most basic level, requires that they be given a reasonable opportunity to understand and respond to the case against them. They claim that natural justice was not afforded to them when they were served with the applicant's submissions on 8 June 2015 given the uncertainty over the funding of US counsel, which was considered necessary due to the applicant making references to US law in its submissions. Such references were not

considered minor or irrelevant and since they were part of the applicant's case the respondents were of the view that they were entitled to investigate the correctness of these references and reply accordingly, but they could not do so without funding to engage US counsel.

### ***Legal Expertise***

#### ***(i) Duty of Candour***

[482] Section 25(3)(a) of the Act specifies that the ROC is admissible as evidence if it is accompanied by an affidavit of an officer of the investigating authority, or the prosecutor, stating among other things that the evidence has been preserved for use in the person's trial. A further requirement under para (b) is that the Attorney-General or principal law officer of the exempted country, as the applicant is in this case, must certify that in his or her opinion the "record of the case discloses the existence of evidence that is sufficient under the law of the exempted country to justify a prosecution in that country."

[483] The respondents submit that they must have the right to establish that both the affidavit and the ROC, or either of them, have not been given in good faith and/or misstate US law. Nothing in the Act prohibits the extradition court from examining the requesting country's certification. English authorities<sup>153</sup> referred to by the respondents stated that the UK magistrates' court has the right to protect its process from abuse and a requesting country has a duty not to abuse that process. The NZ Supreme Court cited with approval this English dicta in *Dotcom v United States of America*.<sup>154</sup>

[484] The assertion by the respondents is that the requesting country owes a duty of candour and good faith to the extradition court. They claim that the United States, as the requesting country in this extradition application, breached that duty of candour and good faith in respect of its evidence on US law and its certification that there is sufficient evidence to justify prosecution of the respondents in the US. In breaching

---

<sup>153</sup> *Knowles v Government of the United States of America* [2007] 1 WLR 47 (PC) and *Wellington v Governor of HMP Belmarsh* [2004] EWHC 418 at [26].

<sup>154</sup> *Dotcom v United States of America* [2014] 1 NZLR 355 at [152], [238] & [293].

that duty the respondents submit that the extradition court would be justified in dismissing the application for extradition.

[485] The respondents submit that the grounds for dismissal are twofold. First, that the certification is flawed therefore the evidence in the ROC is inadmissible and the extradition court will have no evidence before it in order to consider the respondents' eligibility to surrender. Secondly, as an alternative or in combination with the first ground, the duty of candour and good faith is an implied term of the Treaty and given that the duty has been breached by the applicant the respondents' eligibility to surrender should be declined pursuant to s 24(3)(b) of the Act.

(ii) *Extradition Offences*

[486] The applicant submits that the alleged offences are extradition offences under the Act. However, the respondents contend that legal expertise as to the US position at the time the extradition treaty was signed is necessary in order to address the applicant's submissions. This issue arises in relation to the extradition offence of conspiracy to defraud and to the matter of double criminality under s 101B(1)(c) of the Act.

*Conspiracy to Defraud*

[487] In terms of the offence of conspiracy to defraud and the other Treaty offences the respondents seek the assistance of treaty law experts to give evidence as to the relevant intentions of the State Parties to the NZ-US Extradition Treaty at the time the Treaty was signed by the Parties in 1970. Such evidence is needed for the purposes of determining whether there is a prima facie case for the commission of the alleged extradition offences in this case, for Art 31.1 (General Rule of Interpretation) of the Vienna Convention on the Law of Treaties (Vienna Convention) states that:

1. A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.

[488] The respondents submit that comprehending the legal background at the time when New Zealand and the US signed the Treaty is necessary in order to challenge

the applicant's submissions, including those submissions that an offence of conspiracy to commit copyright infringement falls within the ambit of the Treaty offence "conspiracy to defraud".

[489] In addition the applicant, in support of its interpretation of the Treaty, relied on international case-law that pre-dated the execution of the Treaty in 1970. Accordingly the respondents are of the view that in interpreting the offences listed in the Treaty the contemporaneous laws of the Party States is a necessary and primary consideration. It is important to determine what was intended by the drafters of the Treaty when "conspiracy to defraud" was included as an offence in the Treaty to ensure an interpretation consistent with the Vienna Convention. Therefore evidence of the US legal position at the time prior to 1970 is relevant to interpreting the Treaty offences.

#### *Double Criminality*

[490] The matter of double criminality arises due to the effect of the provisions in the TOC Convention. The purpose of TOC, as set out in Art 1, is to promote co-operation between State Parties to prevent and combat transnational organized crime more effectively. The principle of double criminality requires that offences be punishable under the laws of both countries<sup>155</sup>.

[491] Pursuant to Art 34 all State Parties must ensure that their domestic law implements their obligations under TOC. To meet its TOC obligations New Zealand inserted s 101B into the Extradition Act.

[492] Article 16 of TOC deems certain specified offences described in TOC<sup>156</sup> to be included as an extraditable offence in any extradition treaty existing between State Parties. This enables the prosecution of persons, who commit such offences, in more than one State. In addition, particular New Zealand offences may be deemed a "serious offence" under TOC if the 4 years' imprisonment threshold is met and it is submitted the requesting State is able to establish double criminality by reference to "organized criminal group", defined in Art 2(a) of TOC to be:

---

<sup>155</sup> *USA v Cullinane* [2003] 2 NZLR 1 (CA) at [50],

<sup>156</sup> Articles 5, 6, 8 and 23.

A structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit.

[493] Section 101B(1) of the Act deems a list of offences “to be offences described in an extradition treaty”. In reliance on s 101B(1)(c)(i) and (iii), namely that the offences are punishable by a term of 4 years or more imprisonment and that the persons alleged to be involved in an organized criminal group were in New Zealand, the applicant deems the following New Zealand offences as extradition offences under the Treaty:

- section 249 Crimes Act 1961 - Accessing computer system for dishonest purpose;
- section 228 Crimes Act 1961 – Dishonestly taking or using document;
- section 240 Crimes Act 1961 – Obtaining by deception or causing loss by deception;
- section 131 Copyright Act 1994 – Criminal liability for making or dealing with infringing objects;
- section 133 Copyright Act 1994 – Liability of officers of body corporate.

[494] The respondents submit that s 101B(1)(c) introduces a double criminality element into the Treaty in respect of particular deemed offences described therein.

[495] In interpreting s 101B the respondents submit that the applicant’s references to the case of *United States of America v Cullinane*<sup>157</sup> was not authoritative on this issue of double criminality given that *Cullinane* was determined prior to the insertion

---

<sup>157</sup> *United States of America v Cullinane* [2003] 2 NZLR 1 (CA).

of s 101B into the Act.<sup>158</sup> Although the Court of Appeal in *Cullinane* did accept that double criminality would need to be satisfied in respect of some specific offences.<sup>159</sup>

[496] Therefore the respondents submit US counsel is needed to give an analysis on whether the conduct constituting a deemed offence is also punishable under US law. They contend that the double criminality element must be established for one of the particular deemed offences listed before the extradition court can be satisfied that it is an extradition offence.

*(iii) Additional US Expertise*

[497] In the affidavit of Mr Jay Prabhu (the Assistant US District Attorney) that accompanied the ROC, he asserted that he is an expert in the criminal laws and procedures of the US. The applicant's written submissions also made references to US law and to the findings and judgments of the US District Court of the Eastern District of Virginia. The respondents therefore submit that they require access to their own US legal experts in order to review and challenge Mr Prabhu's evidence and the applicant's submissions in order to establish that their evidence and submissions are incorrect or misleading, which would reinforce their argument that the United States has breached its duty of candour in the eligibility proceeding.

[498] Advice from US legal counsel is also sought to provide an analysis and explanation of the applicant's superseding indictment. Such advice is considered necessary in relation to the interpretation of the phrase "the conduct constituting the offence" in s 24(2)(d)(i) of the Act.

[499] The respondents submit that there is a distinction between the terms "the offence" and "the extradition offence" as they appear in the Act, with the former referring to the offence with which the respondents are charged in the US. This advice from US counsel would provide a more balanced view to assist with the Court's understanding of the US offences with which the respondents have been

---

<sup>158</sup> Section 101B of the Extradition Act 1999 was inserted by s 6 of the Extradition Amendment Act 2002 (2002 No 21) and was brought into force, so far as it implemented the UNTOC convention, on 29 September 2003, by clause 2 of the Extradition Amendment Act Commencement Order 2003 (SR 2003/238).

<sup>159</sup> *United States of America v Cullinane* [2003] 2 NZLR 1 (CA) at [61] – [62].

charged and the conduct supporting those charges, rather than to rely solely on the affidavit evidence of the party seeking their surrender for extradition.

***Technical Expertise***

[500] The respondents also wish to call overseas industry practice experts and technical experts to describe the operations and technical infrastructure of Mega and of other similar companies offering cloud storage services. Their evidence would also provide an explanation of Mega's procedure in responding to complaints from copyright holders, clarify the compliance requirements of the DMCA and such evidence would assist in providing relevant and factual context to the Court.

[501] This expert evidence is considered essential by the respondents to counter the applicant's allegations that the Mega websites were operated in such a manner as to provide inferences that the respondents were party to breaches of copyright. The respondents deny that Mega was designed as a platform for downloading or viewing copyright infringing material. They assert that Mega's operations, like other cloud storage websites, were not designed to encourage copyright infringement but were in fact content/copyright neutral.

[502] In particular, it is submitted that technical and industry practice evidence to explain the de-duplication database management system in the uploading of files to website servers, and the removal of URL links rather than the files in response to takedown notices, is necessary to address the allegations of copyright infringing content on Mega's servers and databases.

[503] In addition this expert evidence would also challenge the applicant's candour in the preparation of the ROC and provide assistance to the Court in the assessment of whether there exists a prima facie case of conspiracy or intent to infringe copyright against the respondents.

[504] The respondents submit that the applicant's extradition case against them in respect of these offences is founded on evidence set out in the ROC. From this evidence the Court is requested to draw inferences establishing the appropriate criminal conduct allegedly committed by the respondents. Therefore the



respondents' submit that expert evidence relating to Mega's infrastructure, operations, processes, compliance audits and the general cloud storage industry practice is necessary to raise alternative reasonable inferences.

[505] The possibility of the respondents themselves giving expert evidence exposes them to a challenge by the applicant as to their independence. Further, they say, the right against self-incrimination, protected in the provisions of the New Zealand Bill of Rights Act 1990 (NZBORA) and the Evidence Act 2006, applies to the respondents.

[506] It is submitted that suitably qualified, independent technical experts are not available in New Zealand and the respondents are prevented from engaging such overseas experts as a consequence of the applicant's refusal to provide an assurance that it would not proceed against US experts if they are in receipt of restrained funds released by the NZ High Court by way of fees paid.

### ***Delay & Distraction***

[507] The submission under this heading relates to the conduct of the applicant and Crown Law in the months prior to the commencement of the eligibility hearing so as to delay and distract the respondents from their preparations for the eligibility hearing.

#### ***(i) Delay***

[508] The respondents submit that the direction made by Her Honour Katz J, in her judgment of 1 May 2015<sup>160</sup> to adjourn the 2 June 2015 fixture for the eligibility hearing to a date not earlier than 1 September 2015, acknowledged the respondents' issues in respect of legal representation and funding.

[509] However, they also submit that the extra few months to prepare for the hearing was frustrated by the applicant's tactics in seeking to register the US forfeiture orders in New Zealand during that period, and the lengthy delay in stating its position in relation to US persons and entities receiving monies released by the

---

<sup>160</sup> *Ortmann v The District Court at North Shore* [2015] NZHC 901 at [113].

New Zealand and Hong Kong courts. Consequently the respondents were unable to benefit from the additional time granted by the High Court to advance their preparations for the eligibility hearing and to engage the necessary overseas expertise for the hearing due to the risk of their prosecution in the US.

*(ii) Distraction*

[510] It is submitted that instead of the respondents' legal representatives applying their valuable time and resources to preparing for the eligibility hearing, they were engaged in opposing applications to register the US forfeiture order and to strike out the forfeiture judicial review application, opposing orders permitting the Attorney-General to send to the US items seized from the respondents, making applications to the superior courts to stay the eligibility hearing on the basis of abuse of process by the applicant, and constantly requesting clarification from the applicant as to its position on the respondents' funding.

[511] The respondents submit that these steps taken by the applicant served to distract their counsel from preparation for the forthcoming eligibility hearing.

*Prejudice*

[512] The respondents submit that the applicant carried out successive waves of attack on their financial resources to deprive them of funding to mount a defence to the eligibility application and therefore "starve" them into submission.

[513] Accordingly, they say the applicant's actions were in breach of the following:

- (1) The respondents' right to the observance of the principles of natural justice protected under s 27 of the NZBORA;
- (2) Article IX of the Treaty, which specifies that the determination of extradition must be made in accordance with the laws of the requested country (in this case New Zealand) and the person whose extradition is sought has the right to use such legal remedies and recourses as are provided by such law;

- (3) Article 16.13 of TOC, which provides a guarantee by the State Party of fair treatment to any person who is subject to extradition proceedings in connection with an offence involving an organized criminal group. However, mutual legal assistance may be refused by the requested State Party under Art 18.21 in particular circumstances;
- (4) The judgments of Her Honour Courtney J dated 18 April 2015, Her Honour Katz J dated 1 May 2015 and Her Honour Ellis J dated 3 June 2015, and including various teleconferences with Courtney J in May and June 2015.

[514] As a result of these alleged breaches the respondents say they suffered prejudice in being unable to instruct independent US legal, technical and industry practice experts unless these experts were able to provide their services gratis. In addition their legal teams were deprived of time to prepare for the eligibility hearing. They say their inability to properly defend their position at the eligibility hearing therefore amounted to a breach of natural justice.

### *Abuse of Process*

[515] The actions and conduct of the applicant, the respondents submit, amounts to abuses of process and consequently a fair eligibility hearing cannot be held, which is in breach of the natural justice principles in s 27 of the NZBORA. This breach of natural justice cannot be remedied by the respondents exercising their rights of appeal<sup>161</sup> or taking the matter on judicial review after the eligibility hearing. They submit that the principles of natural justice should be observed at every stage of a proceeding. Since this did not occur in this case the only remedies that can be afforded to the respondents would be for the Court to grant either an interim stay of proceedings until the applicant withdraws its threat to prosecute US persons receiving the released restrained funds, or a permanent stay if this threat is not withdrawn.

---

<sup>161</sup> Extradition Act 1999, s 68 – appeal on question of law only.

### **The Applicant's Submissions**

[516] The applicant, who is the respondent in this stay application, questions the relevance of the respondents' need to call expert evidence from US witnesses. It sees the two principal issues as:

- (1) The extent to which the law of the United States is relevant at the eligibility hearing given that the requesting country need only show a prima facie case that the respondents have committed a treaty offence under New Zealand law or under the New Zealand/United States of America Extradition Treaty
- (2) The relevance of industry practice and technical evidence to the extradition proceeding

#### ***Evidence on the Law of the United States***

[517] That the respondents require access to legal advice on US law is refuted by the applicant, which submits that only one of the 13 charges laid against the respondents does not have an eligibility pathway under s 101B of the Act based on a New Zealand offence. The exercise of applying the respondents' alleged conduct to New Zealand offences does not require reference to US law. Accordingly s 101B does not require the Court to hear argument on the matter of the application of US law to the extradition offences. The Court is invited to conclude that further expertise on US law is not relevant to the extradition proceeding.

#### ***Evidence on Industry Practice & Technology***

[518] The applicant also submits that industry practice and technology evidence is unnecessary since only one strand of evidence is sufficient to find the respondents eligible for surrender. This evidence, the applicant submits, is the implementation of a rewards scheme as an incentive to encourage users to upload files to Mega's servers, which the respondents allegedly knew contained copyright infringing material, and that they knew they were paying for and preserving such infringing content. The respondents allegedly profited from these repeat infringers.

[519] The applicant says the respondents' submissions are vague in regards to technical evidence, and there is no explanation how evidence of cloud storage industry practice affects their eligibility for extradition. Further, the respondents themselves could have given evidence as to the technical operations of Mega and cloud storage systems in general.

[520] In addition the applicant submits that expert evidence on general industry practice will not be of assistance to the Court to demonstrate the alleged manifest unreliability of the ROC, as the applicant has already adduced evidence of the respondents' conversations with each other acknowledging their actions. This industry practice evidence is relevant to trial defences, not to an eligibility proceeding.

[521] The respondents' failure to particularise and relate this expert evidence to specific extracts in the ROC, the applicant submits, means that the respondents have not established that such evidence is relevant to the eligibility proceeding.

### **The Respondents' Evidence**

[522] Three of the respondents, Messrs Ortmann, van der Kolk and Dotcom, and Mr Dotcom's US counsel, Mr Ira Rothken, all gave evidence in support of the stay application.

[523] In his evidence Mr Rothken detailed the various types of legal and technical experts the respondents need in their defence at the eligibility hearing, and the estimated total cost to engage these experts.

[524] The three respondents each described the effect of the US restraining orders on their current financial situations, and they also explained their work, as shareholder employees, in Mega Limited – a company the three respondents established in New Zealand in 2012. Their ability to raise funds is hampered by the lack of a market value for these shares.

[525] The submissions made by the respondents in respect of this first stay application dated 14 July 2015 are thus based upon two premises:

- (1) The respondents should be able to contest the evidence in the record of case by the use of US qualified legal advisors and US based technical expertise; and
- (2) Such legal advice and technical expertise must be paid for and the applicant has prevented the respondents from being able to access such advice and expertise by freezing their overseas funds and by the threat of the seizure of any funds they try to spend outside of New Zealand for such legal advisors and technical experts. The actions of the applicant are deliberately preventing the respondents from accessing evidence they can present at their eligibility hearing in their defence.

### **Onus of Proof**

[526] Under s 24 of the Act, the onus is upon the applicant to present to this Court a prima facie case to establish that the respondents are eligible for extradition. If a prima facie case is established, then under s 24(2) the person is eligible for surrender. This Court must be first satisfied:

- (1) the offence is an extradition offence in the extradition country (the USA);
- (2) the evidence would justify the person's trial if the conduct constituting the offence had occurred in the jurisdiction of New Zealand.

[527] The applicant may submit its evidence by the ROC procedures set out in s 25 of the Act. This Court can be satisfied that an offence is an offence in the extradition country (USA) if a person described in subs (3A) certified that "in his or her opinion the record of case discloses the existence of evidence that is sufficient under the law of the exempted country to justify a prosecution in that country": s 25(3)(b). On the face of the documents the ROC and its supplements have been so certified pursuant to s 25(5), and on the face of it the applicant has established a prima facie case that the alleged offences are extradition offences in the USA.

[528] The respondents are entitled to challenge the correctness of the evidence in the ROC and supplements. It is well established<sup>162</sup> that any challenge to the evidence must be more than simply an alternative explanation. An alternative explanation must be regarded as a trial issue. To successfully challenge a prima facie case once it is established by the ROC requires the respondents to undermine that evidence to the extent that it can be seen to be unreliable and not safe to go to trial.

[529] The principal purpose of this eligibility hearing is as set out in s 24(2)(d), to decide if the evidence in the ROC and supplements would justify the respondent's trial if the conduct constituting the offences had occurred in New Zealand's jurisdiction. This will be considered later in this decision. Nowhere in the Act is it a requirement that this Court should undertake any analysis of the USA offences and applicable law. Those are matters for the Courts in the USA (a case is cited here?).

[530] The submissions made by the respondents in support of the stay application summarised in paras [480] to [514] herein are addressed below, using the same headings.

***Respondents Adequately Understanding and Replying to the Case Against Them***

[531] This eligibility hearing commenced after many delays, on 21 September 2015, over three years and eight months after the respondents' arrests on these matters. They were represented by competent counsel until the latter part of 2014. Since that time, Messrs Dotcom, Ortmann and van der Kolk have been represented by new competent counsel. Mr Batato is self-represented and an Amicus Curiae was appointed to assist him for this hearing. His interests are almost identical to the interests of the other respondents and he has benefitted from their submissions in addition to his own. All respondents have had the applicant's submissions for this hearing since early June 2015. They did not follow the timetable orders set by this Court for the filing of their submissions, and did not do so until this eligibility hearing was underway, and after presentation of the applicant's submissions.

[532] They have had the benefit of previous counsel's research and did not need to wait until the applicant filed its submissions early in June 2015 before they could

---

<sup>162</sup> *USA v Ferras* [2006] SCC 33 (Supreme Court of Canada) at [54].

commence a consideration of their case. They have had successive disclosure of the ROC and its later supplements commencing from early 2012. Most if not all issues likely to arise during this eligibility hearing have been apparent for a long time. They have had over three months to prepare responses to any submissions made by the applicant they might not have anticipated. It is untenable to submit that they have had inadequate time to prepare for this eligibility hearing.

[533] No submission has been made by any of the respondents that the applicant has acted illegally by taking the actions it has to freeze the respondents' overseas assets. No evidence has been produced that questions the certification process of the ROC and supplements. The respondents are arguing that if the applicant released back to the respondents sufficient of the assets the applicant has had legally frozen, then the respondents would be able to pay for legal advisors and technical experts who might produce evidence that would dispute the evidence in the ROC and supplements. At best, that would only provide an alternative point of view as to the correctness of the certification process, the applicable USA law, and on technical matters, all of which are issues for trial.

[534] This stay application is being sought to either stay the eligibility hearing, or to grant an adjournment until the applicant allows the release of money for the respondents to look for evidence that might be useful for their defence trial. This is not a basis for granting a stay.

### ***Legal Expertise***

#### ***(i) Duty of candour***

[535] The respondents are correct when they submit that it must be open to them to show that either or both the affidavit of an officer of the investigating authority (s 25(3)(a) of the Act) and the certificate by a person described in subs (3A), (s 25(3)(b)) have not been given in good faith or misstate the USA law. What they need to go on to show is that there is content in the affidavit or certificate that it is so in error that this eligibility hearing cannot be conducted in a fair manner. That must remain the position unless the certificate is shown to be wrong to the extent that it



would be unfair to conduct this eligibility hearing based upon the ROC evidence covered by that certificate.

[536] It is submitted that the affidavits sworn by Mr Prabhu make assertions as to the USA law which are incorrect. Evidence was given by Mr Rothken and by affidavit by Professor Lessig that they disagreed with Mr Prabhu's view on USA law. It is therefore submitted that the applicant has breached its duty of candour and good faith.

[537] On the evidence in his affidavit, Mr Prabhu appears on the face of it to be well qualified to form the view of USA law that he has expressed. That Mr Rothken and Professor Lessig have a different view of USA law is not sufficient for this Court to disregard the certificate produced pursuant to s 25(5). It is not within the jurisdiction of this Court to rule upon competing views of USA law. That is a matter for trial in the US court. Holding a different view of the law does not amount to bad faith on the part of Mr Prabhu or a breach of the duty of candour, nor does it undermine or invalidate the ROC.

(ii) *Extradition Offences*

*Conspiracy to Defraud*

[538] This issue is whether the Treaty can be interpreted in a manner so that "conspiracy to defraud" includes copyright offending. Article II.16 of the Treaty says:

16. Obtaining property, money or valuable securities by false pretences or by conspiracy to defraud the public or any person by deceit or falsehood or other fraudulent means, whether such deceit or falsehood or any fraudulent means would or would not amount to a false pretence.

[539] In the decision of *USA v Cullinane*<sup>163</sup> Glazebrook J said:

[67] We also refer to the United States Supreme Court decision in *Factor v Laubenheimer* which emphasised the need to give treaties a "liberal" interpretation: "... if a treaty fairly admits of two constructions, one restricting the rights which may be claimed under it, and the other enlarging them, the more liberal construction is to be preferred" (p 293). We note further that s 5(2) of the Extradition Act makes it clear that the

---

<sup>163</sup> *USA v Cullinane* [2003] 2 NZLR 1 (CA).

focus is not on the nomenclature of the offences nor on the constituent elements of the offences. The focus at this stage is whether the totality of the acts or omissions alleged to have been committed comes within the description of the offence in art II, interpreting the words in art II in the manner described above.

[540] In *Edwards v United States of America*<sup>164</sup> Keith J said:

*The approach to interpretation*

[25] We begin with the approach to be adopted to the interpretation of extradition treaties. We were referred to the statements made by Lord Russell of Killowen in *Re Arton (No 2)* [1896] 1 QB 509 at p 517, and oft cited since, for instance at the beginning of this passage from the judgment of Lord Bridge of Harwich in *R v Governor of Ashford Remand Centre, ex p Postlethwaite* [1988] AC 924 at p 947:

“In my judgment these treaties ought to receive a liberal interpretation, which means no more than they should receive their true construction according to their language, object, and intent.’

I also take the judgment in that case as good authority for the proposition that in the application of the principle the court should not, unless constrained by the language used, interpret any extradition treaty in a way which would ‘hinder the working and narrow the operation of most salutary international arrangements.’ The second principle is that an extradition treaty is ‘a contract between two sovereign states and has to be construed as such a contract. It would be a mistake to think that it had to be construed as though it were a domestic statute.’ *Reg v Governor of Ashford Remand Centre, Ex parte Beese* [1973] 1 WLR 969, 973 per Lord Widgery CJ. In applying this second principle, closely related as it is to the first, it must be remembered that the reciprocal rights and obligations which the high contracting parties confer and accept are intended to serve the purpose of bringing to justice those who are guilty of grave crimes committed in either of the contracting states. To apply to extradition treaties the strict canons appropriate to the construction of domestic legislation would often tend to defeat rather than to serve this purpose.”

[541] The decision goes on to say:

[26] The comment might be allowed that the differences suggested 30 or more years ago between the interpretation of domestic legislation and the interpretation of treaties might not now be seen in such sharp terms. Whether that is so or not, the approach to the interpretation of treaties now stated in the Vienna Convention on the Law of Treaties and generally considered to be declaratory of customary international law (for instance by Lord Diplock in *Fothergill v Monarch Airlines Ltd* [1981] AC 251 at pp 282-283) appears to be broadly to the same effect. Under art 31(1):

---

<sup>164</sup> *Edwards v United States of America* [2002] 3 NZLR 222 (CA).

A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.

[27] We see no reason why that “general rule of interpretation” should not be equally applicable to extradition treaties. That approach provides one reason why it is not appropriate to limit the terms of art II by tying them exclusively to the detail of national definitions. So too do the facts that over the life of an extradition treaty (and they tend to have long lives) national definitions will alter; ...

[542] It then goes on to say:

*Its application to the facts*

[28] But to repeat, our task is not to reach a decision solely under the law of one particular jurisdiction. Rather, it is to determine whether the counts as charged do fall within the ordinary meaning of items 14, 15, 16 and 20 in their context and in the light of the treaty’s purpose and object. A primary purpose, emphasised for us by s 12(a) of the Act, must be to fulfil New Zealand’s obligations under the treaty. It is not however a matter of simply using dictionary definitions which, in any event, differ and which must be affected by context. Part of the critical context is that the terms are commonly used for legal purposes, they have legal meanings, even if again those meanings may vary in detail, and the members of the delegations of the two countries who in 1970 prepared the list of property offences included in items 12-20 of art II would have been fully aware of that general legal usage.

[543] In *Scott v Metropolitan Police Commissioner*,<sup>165</sup> the House of Lords held that “conspiracy to defraud” applied in a copyright case where cinematograph films were copied and distributed without the knowledge and consent of copyright owners.

[544] Adopting a liberal interpretation of the Treaty, its purpose, and the rights and obligations of the parties, this Court finds that the counts in the ROC relating to copyright do come within the description of “conspiracy to defraud” in Art II.16 in the Treaty. At best, any US legal evidence that might be obtained by the respondents would only provide an alternative argument which is a matter for trial. It is not a basis for a stay application. It is accepted that pursuant to s 144 Evidence Act expert evidence on USA law is admissible but it has not been shown to be relevant. *USA v McVey*<sup>166</sup> is authority for evidence of foreign law not being admitted by an extradition judge. An extradition judge’s responsibility is to determine whether alleged conduct would constitute a crime if committed in the requested country and

<sup>165</sup> *Scott v Metropolitan Police Commissioner* [1975] AC 819.

<sup>166</sup> *USA v McVey* [1992] 3 SCR 475.

falls within the description of that crime in the Treaty. Evidence of foreign law is not relevant to that process.

*Double Criminality*

[545] A reading of s 101B does not support the respondents' submissions. The relevant portions of s 101B are:

**101B Certain crimes with transnational aspects deemed to be included in extradition treaties**

- (i) For the purposes of this Act and any Order in Council in force under section 15 or section 104, the following offences are deemed to be offences described in any extradition treaty concluded before the commencement of section 6 of the Extradition Amendment Act 2002 and for the time being in force between New Zealand and any foreign country that is a party to a convention or protocol referred to in subsection (5):
  - (a) every offence against any of sections 98A, 98C, 98D, 100, 101, 102, 103, 104, 105, 116, 117, and 243 of the Crimes Act 1961:
  - (b) every offence against any of sections 29A, 30, 30A, 31(1), 31(2) and 32 of the Passports Act 1992:
  - (c) every offence against any enactment if –
    - (i) it is punishable by imprisonment for a term of 4 years or more; and
    - (ii) the offence for which extradition is requested is alleged to involve an organised criminal group (as defined in article 2(a) of the TOC convention); ...

[546] It deems certain crimes with transnational aspects to be part of any extradition treaty and specifies what those offences are in the Crimes Act 1961 and Passports Act 1992. The crimes in those Acts have to be punishable by imprisonment of four years or more and need alleged involvement in an organised criminal group as defined in the TOC convention.

[547] There is no requirement of an extradition court to determine whether the respondents could be tried in the USA. Nothing in s 101B suggests that it should be different from s 24 by importing a double criminality component. To do so would fly in the face of previous authority, particularly *McVey*, which set out the reasons for this:

- 39 The trial judge in the United States, of course, deals with the offence under the law of that country. The identity of that offence can be determined by reference to the text of that law supplied with the requisition. The extradition judge in Canada, on the other hand, is concerned with whether the underlying facts of the charge would, *prima facie*, have constituted a crime listed in the treaty if they had occurred in Canada. That is what is meant by saying that double criminality is conduct based. The courts of both countries deal with the offence under their own law, the law in which they are versed, but each must ascertain whether under that law the facts support the charge.
- 40 I fail to see how proof of foreign law can advance the purpose of the extradition hearing as I have identified it, except possibly in rare cases such as political offences that may be expressly assigned to the extradition judge. On the other hand, to require evidence of foreign law beyond the documents now supplied with the requisition could cripple the operation of the extradition proceedings. It is unthinkable that this would even have been contemplated at the time the Act was passed and many of the existing treaties were negotiated. To transport witnesses, sometimes halfway across the world, would have seemed an impossible prospect. Quite different reasons argue against the possibility in modern times. In our days, crime does not stop at the border. Much of organized crime is international in scope. And as this court noted in *United States v Cotroni* [1989] 1 SCR 1469, 48 CCC (3d) 193, 96 NR 321, 23 QAC 182, 42 CRR 101, at p 1485 [SCR]: “The only respect paid by the international criminal community to national boundaries is when these can serve as a means to frustrate the efforts of law enforcement and judicial authorities.” This criminal community would certainly welcome the need to prove foreign law. Flying witnesses in to engage in abstruse debates about legal issues arising in a legal system with which the judge is unfamiliar is a certain recipe for delay and confusion to no useful purpose, particularly if one contemplates the joys of translation and the entirely different structure of foreign systems of law. In his book *Extradition in International Law* (1971), Shearer thus puts the matter, at pp 139-40:

... it would seem wrong in principle that extradition should be subjected to the unnecessary additional hazard of proof of criminality according to a law unfamiliar to the court before which the fugitive is brought. The true purposes of the double criminality rule are adequately served by the enquiry which the court in the requested State is competent to carry out, viz. the determination whether the act for which extradition is claimed, if committed in the requested State, would constitute an offence under the law of that State.

Lord Ackner expressed his view in this manner in *Sinclair, supra*, at p 91:

Your Lordships are concerned with the construction of an Act passed over a hundred years ago. I cannot accept that the legislature intended that it was to be part of the function of the [extradition judge] to preside over lengthy proceedings occupying weeks, and on occasions months, of his time hearing heavily contested evidence of foreign law directed to whether there had been due compliance with the many and varied obligations of the relevant Treaty. The

inconvenience of such a procedure is well demonstrated by the current litigation.

The same can be said of the present litigation. Subject to the possible exceptional circumstance of political offences to which I have previously referred, I agree with Lord Ackner (quoting Robert Goff LJ) that the extradition judge “is not concerned with foreign law at all” (p 84).

[548] The role of this extradition court is to determine whether the alleged conduct falls within s 101B as that conduct is defined in TOC. The assessment is of criminality against offences in New Zealand under s 101B, and not an assessment of USA law.

*(iii) Additional US Expertise*

[549] The respondents’ submissions under this heading are but a variation of the same theme that the respondents are entitled to USA legal expertise to examine the USA offences. To grant a stay or an adjournment to allow the respondents time and money to analyse the evidence and legal views of Mr Prabhu due to a perceived possibility that they might show that the applicant has breached its duty of candour, is to ignore s 25(5). There is only the views of respondents’ witnesses that disagree with Mr Prabhu’s assessment of USA law. That is a trial issue. If these circumstances were sufficient to grant a stay or an adjournment, every eligibility hearing would qualify for the same remedy. The authorities previously cited above make it clear that is not the case.

[550] In addition, this Court is being asked to:

- (i) Overlook that a Grand Jury has issued an indictment for the respondents; and
- (ii) Assume that the prosecutor may have incompetently or dishonestly brought the charges; and
- (iii) Find the Federal Court of USA had misapplied American law; and
- (iv) Overlook the comity required between the Treaty partners to give effect to their treaties.

There has been a basis established for this Court to do so.

### ***Technical Expertise***

[551] The respondents' submissions, if taken at their highest, is to say that if experts in industry practice and upon technical matters could be engaged by them, then evidence might be provided to the eligibility hearing that could provide alternative explanations relating to the operations of Mega that are necessary to raise alternative reasonable inferences. Briefly stated, an innocent explanation might be given to the evidence from which the applicant draws an inference of criminal behaviour.

[552] An alternative innocent explanation is not enough for this eligibility court to grant a stay or an adjournment. It is not the role of this court to weigh the merits of the applicant's case against the possible alternative explanations that might be provided by the respondents. That is the role of the trial court. Unless the evidence of the respondents is likely to undermine the evidence of the applicant so it can be seen to be manifestly unreliable, a stay or an adjournment to look for this evidence should not be granted. The role of this eligibility court is to assess whether the applicant has established a prima facie case, as persons should not otherwise be subjected to extradition. Provided there is sufficient evidence to show that the respondents could be convicted at a trial, that is sufficient. It is a safeguard against extradition for unmeritorious reasons that do not have a legal basis if the same charges were laid against the respondents in New Zealand law.

[553] The role of an extradition court is encapsulated in the Canadian case *United States of America v Mach*,<sup>167</sup> which said:

## **B. The Jurisdiction of a Judge under section 29**

### **B.1 Introduction**

Before I summarize the evidence in this application and determine its sufficiency under s 29 of the Act, it is helpful to begin with a summary of the jurisdiction of the Court in such an application.

---

<sup>167</sup> *United States of America v Mach* [2006] ONSC 4832.

## B.2 The Recent Developments in the Law

In *United States of America v Ferras*; *United States of America v Latty*, [2006] SCJ No 33, McLachlin CJC reviewed the process for extraditing a person to face charges in a foreign country, that is, the judicial stage under s 29 of the Act, and the executive stage, and focused upon the judicial stage. She emphasized the history of extradition and its dual purposes, saying in paras 21, 22 and 23:

These propositions capture not only the history of extradition, but its dual purposes. The first purpose is to foster efficient extradition where such a case is made out, in accordance with Canada's international obligations. This requires a flexible, non-technical approach. The second purpose is to protect an individual in Canada from deportation in the absence of at least a *prima facie* case that he or she committed the offence alleged, which must also be an offence in Canada. The two purposes are complementary. International comity does not require the extradition of a person on demand or surmise. Nor does basic fairness to the person sought for extradition require all the procedural safeguards of a trial, provided the material establishes a case sufficient to put the person on trial.

The meaningful judicial process just described involves three related requirements: a separate and independent judicial phase; an impartial judge or magistrate; and a fair and meaningful hearing.

[554] The respondents are entitled to challenge the applicant's evidence in the ROC at this eligibility hearing. How this court should assess such a challenge is described in a Canadian case *United States of America v Ferras*:<sup>168</sup>

54. Challenging the justification for committal may involve adducing evidence or making arguments on whether the evidence could be believed by a reasonable jury. Where such evidence is adduced or such arguments are raised, an extradition judge may engage in a limited weighing of evidence to determine whether there is a plausible case. The ultimate assessment of reliability is still left for the trial where guilt and innocence are at issue. However, the extradition judge looks at the whole of the evidence presented at the extradition hearing and determines whether it discloses a case on which a jury could convict. If the evidence is so defective or appears so unreliable that the judge concludes it would be dangerous or unsafe to convict, then the case should not go to a jury and is therefore not sufficient to meet the tests for committal.

[555] In New Zealand the Court of Appeal said in *United States of America v Dotcom*:<sup>169</sup>

<sup>168</sup> *United States of America v Ferras* [2006] 2 SCR 77.

<sup>169</sup> *United States of America v Dotcom* [2013] 2 NZLR 139 (CA).



[108] Finally, as we noted earlier, the record of the case procedure is an “on the papers” process as far as the requesting state is concerned. There can be no sensible expectation that a requesting state such as the United States will have potential trial witnesses available in New Zealand for an extradition hearing. This affects the extent of the evaluation that the extradition court can conduct and the nature of the evidence that the suspect can reasonably expect to present. The role of the extradition court is, as the Canadian and United Kingdom courts have repeatedly said, a limited one. In this context, it is to ensure that the requesting state has presented sufficient evidence to indicate that there is a prima facie case against the suspect. A suspect may well be able to point to gaps or flaws in the material summarised or analysed in the record of the case, or may be able to point to documentary or other evidence which causes the extradition court to doubt the reliability of the material proffered by the requesting state. This may cause the extradition court to conclude that the requesting state has not established a prima facie case. But a challenge which does not go to the reliability of the material in the record but to its interpretation – that is, to the inferences that should be taken from it – is more appropriate to trial than to an extradition hearing.

[556] A competing explanation of the applicant’s evidence is not a sufficient basis for granting a stay. The respondents’ challenge must go to the reliability of the ROC. This is expressed in *United States of America v Aneja*:<sup>170</sup>

[48] As interpreted in *Anderson and Thomlison*, s 29(1)(a) provides for a limited review of the evidence. Where the ROC on its face justifies committal for surrender, the subject of extradition can successfully challenge that evidence only by showing that some part or parts of the ROC essential to committal should be completely rejected as unreliable. It is not enough to show that there is good cause to doubt the reliability of some part of the ROC, or that evidence relied on in the ROC might well be eventually rejected at trial...

[557] The first respondent did produce an expert witness, Philip Sallis, a professor of computer science at AUT University. His evidence was instructive and useful as to the technical operations of the internet and the cloud storage. His evidence also provided an alternative explanation to some of the evidence in the ROC. However, it did not undermine that evidence and show it to be unreliable. At best, it offered an alternative explanation that could be relevant at trial.

[558] For the second and third respondents it is submitted that only experts based in the USA have the expertise to challenge the evidence in the ROC. That is a bare submission unsupported by evidence. Professor Sallis was not asked if this was so,

---

<sup>170</sup> *United States of America v Aneja* (2014) 113 WCB 423 (ONCA).

and it could be assumed that, as an expert in this area himself, he might well know. There is no evidence to suggest that if such experts were consulted, they would undermine the ROC to the extent that it would be apparently unreliable. Counsel for the second and third respondents submitted that this evidence was necessary to raise alternative reasonable inferences, and if that is all that is expected to be adduced, then it is a trial matter and not relevant to this eligibility hearing.

[559] It is submitted that the expert evidence of USA based experts would also challenge the applicant's candour in its ROC. This is largely a rerunning of the disclosure case decided upon by our Supreme Court in *Dotcom v USA*.<sup>171</sup> In that case, it was said:

[147] In short, the legislative history of s 25 does not support the view that it is mandatory for the record of the case to include copies of all documents relevant to the requesting country's case. Such an approach would involve treating s 25 as if it imposed a disclosure regime, albeit one particular to proceedings in which the record of case procedure is invoked. An obligation to include all relevant documents would be so onerous in a case of any complexity that requesting state would be discouraged from using the record of case procedure. By contrast, the very purpose of the record of case process was to simplify the presentation of evidence by the requesting state, as is evident from its origins and development as discussed above.

#### **The duty of candour**

[148] The appellants also referred in their submissions to decisions of English courts and the Privy Council establishing that a requesting state owes a common law duty of candour to the extradition court. In 1993, in *R v Governor of Pentonville Prison, ex parte Lee*, the Divisional Court held that the requesting state was to be the "sole arbiter" of the material that it may choose to place before the extradition court. The requesting state had no general duty of disclosure, for that would be incompatible with the nature of extradition, which was a creature of statute. Nor did the extradition court have any right or power to request further material from a requesting state. The Court observed, however, that extradition legislation was based on the assumption that the requesting state was acting in good faith.

...

[150] This "general duty on a requesting state to be candid about vitiating factors in its case" was also referred to by Sedley LJ, giving judgment for himself and Pitchers J in the Administrative Court in *Jenkins v Government of the United States of America*. In 2006, in *Knowles v*

---

<sup>171</sup> *Dotcom v USA* [2014] 1 NZLR 355 (SC).

*Government of the United States of America*, Lord Bingham, on behalf of the Privy Council, summarised the principles which had merged from the earlier cases:

There are many respects in which extradition proceedings must, to be lawful, be fairly conducted. But a requesting state is not under any general duty of disclosure similar to that imposed on a prosecutor in English criminal proceedings. It does, however, owe the court of the requested state a duty of candour and good faith. While it is for the requesting state to decide what evidence it will rely on to seek a committal, it must in pursuance of that duty disclose evidence which destroys or very seriously undermines the evidence on which it relies. It is for the party seeking to resist an order to establish a breach of duty by the requesting state.

...

[152] The approach taken by the Privy Council in *Knowles* should be applied in New Zealand. The scheme of Part 3 of the Extradition Act is based on an assumption that requesting states that are exempted countries are in general to be taken on trust in relation to the contents of the record of the case that they submit. Requesting states, however, owe a duty of candour and good faith to the extradition court. They must disclose any evidence that would render worthless, undermine or seriously detract from the evidence upon which they rely, whether on its own or in combination with material that is in the requesting state's possession or is drawn to its attention by the requested persons or the Court. The record of the case process does not diminish that duty and requesting states must accordingly include any such material in the record of the case or a supplement. The New Zealand authorities or agencies that are assisting or acting on behalf of requesting states have a correlative duty to the court to use their own best endeavours to ensure that requesting states comply with their obligations in this respect.

...

[161] It is helpful to consider whether, without disclosure, the present appellants are able to participate in a meaningful way in the extradition hearing. The case against them turns largely on the design and operation of the Megaupload business model and associated inferences. The appellants must be well aware of the detail of the business model and the way it operated. It was accepted that they have general access to their own email accounts and financial information. They have also been given a copy of the Megaupload server databases. Importantly, we were not advised of any specific respects in which they lack the information they need to contradict or challenge assertions made in the record of the case, or to advance innocent explanations for the allegations against them. They have thus failed to particularise any tangible disadvantages which they will face if denied disclosure. So, to the extent to which their personal circumstances may require consideration, the appellants have failed to establish that ordering disclosure is necessary to ensure that they have a fair extradition hearing. There is, accordingly, no basis on which the District Court in the present case could exercise any inherent power to order disclosure. ...

[560] In summary:

1. The applicant is not required to produce all the evidence in the ROC it has available to it;
2. It is not required to produce evidence which might be useful to the respondents;
3. It does have a duty of candour and good faith to produce evidence which might destroy or seriously undermine the ROC;
4. The respondents have not established a breach of the duty by the applicant. At best, it is submitting an alternative explanation that might be available, which is a trial matter; and
5. A stay or an adjournment should not be granted for the claimed need for technical expertise.

### ***Delay & Distraction***

#### ***(i) Delay***

[561] This submission is substantially covered by paras [508]-[509] herein. The respondents' submissions based upon the decision of Her Honour Katz J in *Ortmann & Ors v The District Court at North Shore*<sup>172</sup> are selective. Her Honour concluded:

[118] I have therefore concluded, with some reluctance (given the time that has elapsed since the plaintiffs were first brought before the Courts) that the interests of natural justice require an adjournment of the 2 June 2015 extradition hearing date. This should not be taken by the plaintiffs, however, as a signal that any ongoing funding or representation difficulties (if they arise) would be likely to justify further adjournments. On the contrary, the plaintiffs must take full responsibility for preparing for their extradition hearing on whatever new date is allocated, with whatever level of legal support they are able to secure. For the reasons I have outlined in relation to Mr Batato, even if all of the plaintiffs were to be self-represented, it would not automatically follow that the requirements of natural justice could not be met at a future hearing.

---

<sup>172</sup> *Ortmann & Ors v The District Court at North Shore* [2015] NZHC 901.

[562] The respondents have had other litigation pending since the decision of Katz J, some of it initiated by themselves. Nevertheless, I am satisfied that the respondents have had more than sufficient time and resources to prepare for this eligibility hearing if they were so minded.

(ii) *Distraction*

[563] The same reasons apply as set out in paras [510] to [511] above. There is no barrier for a stay or adjournment of the eligibility hearing on the basis of alleged delay or distraction as submitted.

*Prejudice*

[564] The grounds for a stay submitted here are substantially a compilation of the other grounds already advanced. When they are all considered together it is submitted that the respondents' rights under the NZBORA, s 27, have been breached and they have not had the benefit of fair treatment guaranteed under Art 16.13 of the Treaty.

[565] Both grounds appear to be based upon what the respondents describe as a wave of attacks on their financial resources to "starve" them into submission at this eligibility hearing. There has been no evidence of such intent adduced at this hearing to back up those allegations, nor has it been shown that any of the legal steps taken by the applicant were wrongly taken so as to achieve the alleged purpose. The respondents have also brought legal proceedings in respect of these matters which they are equally entitled to do. There has been no evidence that they have been starved of funds. There is evidence of funds being released to the respondents for the funding of their legal defence through decisions made by the High Court. They have had funding available to them far above and beyond the funding that most litigants would have available to them. There is no merit in these submissions that would justify a stay.

*Abuse of Process*

[566] The respondents submit that an eligibility hearing can be stayed where:

- (1) It is impossible for the requested person to receive a fair eligibility hearing; and
- (2) Allowing the eligibility hearing to take place would undermine public confidence in the integrity of the criminal justice system.

[567] The submissions that they have been denied a reasonable opportunity to prepare a defence, that they have been precluded from being heard on all issues including US law, and that they cannot call witnesses with expertise in US law and technology have all been considered earlier in this judgment.

[568] The respondents also submit that if the eligibility hearing results in a finding that the respondents are eligible for extradition, then their rights will be prejudiced as under Part 8 of the Act, their rights of appeal are restricted to matters of law. Also, appeal rights could be lengthy and the respondents might be deprived of their liberty during that process. They fail to explain how this Court should ignore the provisions of the Act and grant a stay because of the risk of an adverse decision to the respondents from this hearing.

[569] The respondents submit that public confidence in the integrity of the criminal justice system would be undermined if a stay was not granted. They submit that the joint search and seizure operation carried out in January 2012 was carried out on a scale and intensity unprecedented in New Zealand. The applicant has also had full access to the New Zealand legal system to advance its objectives, including the advantage provided to the applicant by having a privileged status under MACMA and the Act.

[570] As already noted in this judgment the arrests and seizure in January 2012 are already the subject of proceedings in the High Court brought by the first respondent. Those events happened years ago and do not affect the fairness of this hearing. Whatever advantages it is perceived the applicant might have pursuant to MACMA and the Act are those legitimately available to them. They are not a basis for a stay application. Granting a stay application based on these submissions with total

disregard for the law is more likely to undermine public confidence in the criminal justice system than it is to proceed with this eligibility hearing to a conclusion.

### ***Conclusion***

[571] There is no basis for granting this application for a stay for any of the submissions advanced either individually or when considered collectively.

### **Stay Applications 2 and 3**

[572] On 21 October 2015 the applicant filed a preliminary objection to stay applications 2 and 3 (dated 21 August and 16 September 2015) filed for the first respondent, Mr Dotcom. Full submissions were heard on this objection prior to commencing a hearing of these stay applications.

[573] The applicant submits that the stay applications have no direct connection with the Court's function under s 24, or do not affect the fairness of the hearing. The applicant contends that the stay applications do not lie within the jurisdiction of this extradition Court and, even if they did, they do not come up to the high threshold for staying the eligibility hearing.

[574] The first respondent confirmed that the Amended Application by the First Named Respondent for an Order Staying the Proceedings of 16 September 2015 includes the grounds for the stay application of 21 August 2015 and can be considered together. The general ground of the stay application is the alleged abuse of process by the applicant. The first respondent submits that in the circumstances, allowing the eligibility hearing to take place would undermine public confidence in the integrity of the New Zealand criminal justice system, as described in *R v Antonievic*.<sup>173</sup> This application is supported by the other respondents and they submit that the eligibility hearing should also be stayed against them.

[575] The first respondent seeks orders:

1. Granting a permanent stay in respect of all proceedings brought by the applicant against the first respondent in these proceedings;

---

<sup>173</sup> *R v Antonievic* [2013] 3 NZLR 806 (CA) at [48(b)].

2. Discharging the first respondent from his obligations in respect of bail in these proceedings;
3. Addressing such further or incidental matters in respect of these proceedings as may be just;
4. Reserving costs.

[576] In the alternative, the first respondent applies to the Court for orders:

1. Granting an interim stay of these proceedings pending the conclusion of proceeding number CIV-2013-404-2168 (the *GCSB* proceeding);
2. Reserving costs on this application.

[577] The orders sought are based on the grounds that there has been an abuse of process by means and manner by which the applicant and/or others acting on behalf of the applicant (whether as agents or otherwise) have:

- (a) Commenced prosecution due to political considerations;
- (b) Granted residence to the first respondent in New Zealand contrary to standard immigration policy in order to provide a pathway to extradition;
- (c) Proceeded by way of an *ex parte* application (without notice) to stop the trading of a number of businesses associated with the first respondent;
- (d) Proceeded by way of an *ex parte* application to restrain the assets of the first respondent and of individuals associated to the first respondent;
- (e) Pursuant to that *ex parte* application, sought a global restraint of assets to deliberately prevent the first respondent from being able to properly contest the eligibility hearing in New Zealand;



- (f) Pursuant to that *ex parte* application, sought global restraint of assets to deliberately prevent the first respondent from being able to properly fund a defence of the allegations in the United States of America;
- (g) Asserted extra-territorial jurisdiction unilaterally in an attempt to regulate the internet contrary to the global public interest which is inconsistent with a free and open internet;
- (h) Gathered intelligence and/or investigative material relating to the first respondent;
- (i) Denied the first respondent access to exculpatory material;
- (j) Breached its duty to preserve evidence and then frustrated the attempts of the first respondent and/or Megaupload Limited to preserve that evidence;
- (k) Pursued the arrest and extradition of the first respondent under the provisions of the Act;
- (l) Taken steps against the first respondent purportedly pursuant to MACMA;
- (m) Publicly humiliated the first respondent and members of his family;
- (n) Traumatized the children of and under the care of the first respondent contrary to their best interests;
- (o) Engaged in collateral or related litigation both in New Zealand and overseas; and
- (p) Otherwise conducted themselves in relation to these proceedings.

[578] The grounds alleging an abuse of process in the paragraph above are considered below using the same subparagraph numbers:

- a. The allegation that the respondents are being prosecuted due to political considerations is based upon an assertion by the first respondent that this is the case. This Court is asked to draw an inference that this is the case due to donations made to political parties in the USA by media companies and persons claiming to be adversely affected by Mega, and various meetings between those persons and highly placed politicians, including the President and Vice President of the USA. The donations by media companies to the major political parties (both the Democrats and Republican parties) in the USA, and the meetings between executives of those companies and politicians may well have other explanations than those attributed by the first respondent. There is no direct evidence of a linkage to the donations and those meetings with the applicant to extradite the respondents. Even if there was, if law enforcement agencies in the USA were of the view that crimes had been committed by the respondents, for which they could stand trial in the USA, they are entitled to seek their extradition notwithstanding the initial impetus to prosecute. Their motives to seek extradition do not potentially affect the fairness of this eligibility hearing and there is not a ground to grant a stay application.
- b. This allegation has already been the subject of a decision of this Court on 23 May 2014<sup>174</sup> and the High Court on 17 October 2014<sup>175</sup> where it was found that there was no evidential linkage between the granting of residence to the first respondent and these eligibility proceedings. There is no new evidence to change these findings and it was a pointless exercise seeking a stay of the eligibility hearing on this ground.
- c. d. e. and f are considered together. This Court has already found earlier in this decision that the respondents having access to funds to employ legal experts in the USA to give evidence at this eligibility hearing on USA law is not necessary or relevant for this Court to conduct this

---

<sup>174</sup> *USA v Dotcom* (North Shore DC, CRI 2012-092-1647, 23 May 2014, Judge Dawson).

<sup>175</sup> *Dotcom v USA* [2014] NZHC 2550 (Simon France J).

eligibility hearing. The conduct alleged is clearly identifiable and has occurred. The conduct that has been alleged does not prevent this Court from conducting a fair eligibility hearing.

- g. If correct or not, this allegation has no relevance to the conduct of a fair eligibility hearing.
- h. As in subparagraph (b) above these allegations have already been dealt with by this Court<sup>176</sup> and the High Court.<sup>177</sup> No evidence has been adduced that would change those decisions and nor do they adversely affect the conduct of a fair eligibility hearing. If this ground purports to relate to the unlawful gathering of evidence by the GCSB, then it is noted that this has already been before the High Court (CIV-2013-404-2168) and it is appropriate for this issue to remain there. It is not appropriate for this Court to take over this matter and reach any decision upon it. Any allegation of illegality or improperly gained evidence by the applicant or its agents is a trial issue, not an eligibility hearing issue.
- i. It is not clear from the first respondent's application and submissions but it would appear that this ground of alleged abuse of process is based upon the seizure of the first respondent's computer-based information and data. This data has since been cloned and made available to the first respondent for a considerable time prior to this eligibility hearing. This ground is a trial issue and does not prevent the conduct of a fair eligibility hearing.
- j. As in subpara (i) above, this is a trial issue and does not prevent a fair eligibility hearing.

---

<sup>176</sup> *USA v Dotcom* (North Shore DC, CRI 2012-092-1647, 23 May 2014, Judge Dawson).

<sup>177</sup> *Dotcom v USA* [2014] NZHC 2550 (Simon France J).

- k. The methods and tactics used by authorities to arrest the first respondent and the following processes are not relevant to an eligibility hearing and nor do they impact upon the fairness of the hearing.
- l. The steps taken by the authorities pursuant to the MACMA are alleged to amount to an abuse of process have not been shown to have impacted upon the conduct of a fair extradition hearing.
- m and n. The alleged public humiliation of the first respondent and his family and the alleged trauma to their children do not amount to an abuse of process affecting the fair conduct of this eligibility hearing.
- o. There is no evidence that collateral or related litigation in New Zealand or overseas has affected the fair conduct of this eligibility hearing. Any such litigation will be heard and decided upon by those Courts. It is not appropriate, and nor does this Court have the jurisdiction, to intervene.
- p. It is not clear from the first respondent's submission but it is assumed that this ground relates to the allegation of an apparent conflict of interest arising out of the Crown Law Office. It is submitted that the application through the Crown Law Office seeking the extradition of the first respondent while the official New Zealand agencies need only to comply with their obligations under the Privacy Act 1993 and/or the Official Information Act 1992 results in a conflict of interest. It is alleged that these are two sets of interests which potentially conflict, and with an apparent conflict of interest then there cannot be public confidence that the Crown Law Office will process requests in an expeditious, efficient and correct manner. It is a bare allegation of conflict. No evidence has been adduced to show any actual conflict. There are occasions when an apparent conflict can of itself mean that it is safer for a legal representative to withdraw to preserve the appearance of fairness. This is not one of those occasions. It is an allegation easily made and is not made on the basis of any evidence whatsoever. If the submission were to be accepted, it would be

tantamount to saying that the Crown Law Office cannot act for any government agency, which is an absurdity given the purpose of the Crown Law Office. This allegation does not lead to any finding that this eligibility hearing was not conducted in a fair manner.

[579] None of the abuse of process grounds raised in the first respondent's application leads this Court to decide that this eligibility hearing is not a fair hearing. The applications are therefore declined.

## **PART C**

### **Eligibility Hearing**

#### **Legal Background**

[580] In order for the respondents to be eligible for surrender this Court must first be satisfied that the alleged conduct amounting to US offences are extradition offences. The alleged conduct in each count needs to translate into an extradition offence by way of either:

- (1) Article II of the Treaty (i.e. an offence originally listed in the Treaty);
- (2) Section 101B(1)(a) of the Act (a deemed extradition offence); or
- (3) Section 101B(1)(c) (a deemed extradition offence involving an organised criminal group as defined in Art 2(a) of TOC).

[581] Pursuant to s 11, the Act is to be construed to give effect to the Treaty. The applicant is an exempted country pursuant to s 17 of the Act and under s 25(1) is able to present its evidence by a ROC.

[582] This Court must first decide if the extradition is being sought for alleged offences that are extradition offences: s 24(1). Then this Court needs to establish whether a prima facie case has been established in respect of the extradition offence: s 24(2)(d)(i).

## **Standard of Proof**

[583] The necessary standard of proof is discussed at [16]-[21] of this decision.

### **Counts:**

#### **Count 2: Conspiracy to Commit Copyright Infringement**

[584] It is convenient to commence by considering Count 2 first. In this count the alleged unlawful conduct involves the respondents conspiring to operate the Mega business as a vehicle for downloading or viewing copyright infringing material for the purpose of financial gain. The applicant submits that this charge corresponds with Art II.16 of the Treaty, which grants extradition in respect of the following offence:

16. Obtaining ... money ... by conspiracy to defraud the public or any person by ... fraudulent means, whether such ... fraudulent means would or would not amount to a false pretence.

[585] To satisfy the conduct requirement of the offence described in Art II.16 there must be prima facie evidence of an agreement to obtain money by dishonestly depriving copyright owners of their propriety rights.

[586] Deceit of the defrauded party is not a necessary element of the Treaty offence, the applicant need only show that the person will be dishonestly deprived. This might occur through the fraudulent interference with another's proprietary right, such as the copyright to a film, music, or literary work.

[587] The applicant further submits that count 2 corresponds also with the following New Zealand offences, charged as conspiracy offences:

- Section 249 Crimes Act 1961 – Accessing computer system for dishonest purpose;
- Section 228 Crimes Act 1961 – Dishonestly taking or using document;

- Section 131 Copyright Act 1994 – Criminal liability for making or dealing with infringing objects.

These are offences deemed under s 101B of the Act to be included in the Treaty.

***Count 2: Treaty Article II.16***

[588] There is an abundance of evidence that Mr Ortmann and Mr van der Kolk administered a rewards programme for the Mega group from September 2004 until July 2011. This enabled subscribers to earn rewards, including cash payments, if there was a high level of traffic through the URL links associated with their accounts. This operated as an incentive to upload popular works and to post links on third party linking sites so they would be widely accessible. There is also an abundance of evidence in the ROC that works that infringed the right of copyright owners were uploaded and in demand. There is evidence that traffic to copyright infringing material substantially drove the growth of the Mega business and this was known and encouraged by Messrs Ortmann, van der Kolk, and Dotcom. It can be inferred that Mr Batato had knowledge of the Mega business model and participated in a conspiracy through promoting the Mega business as its marketing manager.

[589] There is a prima facie case that the respondents did share a common intention to:

- (i) obtain popular content knowing that much of it was infringing content by offering rewards;
- (ii) encourage widespread access to that material by rewarding uploaders for the traffic they generated; and
- (iii) maintain the availability of copyright infringing content.

[590] There is evidence that the Mega businesses obtained large profits (passed on to the respondents by their respective drawings) from the unauthorised use of copyright content which prejudiced the property rights of the copyright owners.

There is evidence that the respondents knew that the copyright owners were so prejudiced.

[591] Inferences can be drawn from the evidence that Messrs Dotcom, Ortmann and van der Kolk agreed:

1. They would attract popular copyright infringing files by offering rewards;
2. They would pay uploaders whose content attracted substantial traffic, irrespective of whether that content infringed copyright;
3. They would fix free viewing times on Megavideo with a view to exploiting the popularity of commercial movies subject to copyright, thereby maximising the incentive to purchase subscriptions;
4. They would not delete or remove all access to files subject to DMCA takedown notices;
5. They would disguise the hosting of infringing files by manipulating the front pages of their sites, suppressing the identities of users on public pages, concealing the hosting of videos longer than 10 minutes, and populating Megavideo front pages with user-generated content unlawfully reproduced from YouTube;
6. They would conduct their auditing procedures to allow infringing content to be hosted;
7. They would take steps to frustrate the “justice system” in the event of legal action against them;
8. They would expedite the mass distribution of infringing files by copying the most popular content to Cogent servers and converting video files into a form which enabled more rapid distribution;



9. They would showcase the availability of high definition copyright movies;
10. They would frustrate the efforts of copyright owners to have infringing content taken down;
11. They would deceive copyright owners about the action they took in response to takedown notices;
12. They would encourage the activities of repeat infringers and shelter them from detection by copyright owners; and
13. They would disguise the hosting of infringing content by making Megaupload non-searchable and strictly limiting the searchability of the Megavideo site. At the same time, they would exploit third party linking sites as a means of making infringing content available to internet users.

[592] It can also be inferred that Mr Batato joined the business in 2007 and:

1. Participated with knowledge that Mega unlawfully exploited traffic to the large volumes of infringing content it hosted;
2. Appreciated that Mega needed to conceal the extent of infringing content it hosted, by restricting or preventing direct searching of its holdings;
3. Appreciated that traffic to infringing content was conducted on a large scale through the medium of third party linking sites;
4. Encouraged users to find infringing content using third party linking sites;
5. Directly advanced the conspiracy by selling Megaclick advertising to websites he knew were engaged in copyright infringement; and

6. Assisted the activities of repeat infringers by providing them with advertising services on Mega sites.

[593] There is evidence of conduct from which it may be reasonably inferred that each of the respondents was a member of this conspiracy. Mr Batato joined the Mega business after the time the applicant alleges the conspiracy began. That does not exculpate Mr Batato as there is evidence of conduct from which it may reasonably be inferred that he joined the conspiracy after it was already operating. He may have played a smaller role than the other respondents but that does not exclude him from the alleged offending. The evidence is sufficient to find that a prima facie case is established against each of the respondents on count 2 under Art II.16 of the Treaty and the respondents accordingly eligible for surrender on count 2.

***Count 2: Section 249 Crimes Act 1961***

[594] Section 101B of the Act provides:

**101B Certain crimes with transnational aspects deemed to be included in extradition treaties**

- (i) For the purposes of this Act and any Order in Council in force under section 15 or section 104, the following offences are deemed to be offences described in any extradition treaty concluded before the commencement of section 6 of the Extradition Amendment Act 2002 and for the time being in force between New Zealand and any foreign country that is a party to a convention or protocol referred to in subsection (5):
  - (a) every offence against any of sections 98A, 98C, 98D, 100, 101, 102, 103, 104, 105, 116, 117, and 243 of the Crimes Act 1961:
  - (b) every offence against any of sections 29A, 30, 30A, 31(1), 31(2) and 32 of the Passports Act 1992:
  - (c) every offence against any enactment if –
    - (i) it is punishable by imprisonment for a term of 4 years or more; and
    - (ii) the offence for which extradition is requested is alleged to involve an organised criminal group (as defined in article 2(a) of the TOC convention); ...

[595] Subsection (5) says:

(5) For the purposes of this section,-

...

**TOC convention** means the United Nations Convention against Transnational Organised Crime, done at New York on 15 November 2000.

[596] The USA and New Zealand are both parties to TOC. Any offence encapsulated by s 101B(1)(c) is deemed to be an offence under the Treaty.

[597] Section 249 Crimes Act 1961 provides:

**249 Accessing computer system for dishonest purpose**

- (1) Every one is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly, accesses any computer system and thereby, dishonestly or by deception, and without claim of right,-
  - (a) obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or
  - (b) causes loss to any other person.
- (2) Every one is liable to imprisonment for a term not exceeding 5 years who, directly or indirectly, access any computer system with intent, dishonestly or by deception, and without claim of right,-
  - (a) to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or
  - (b) to cause loss to any other person.
- (3) In this section, deception has the same meaning as in section 240(2).

[598] Under s 248 of the Crimes Act 1961 “access” is defined to mean “in relation to any computer system ... communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system. The section also defines “computer system”:

**Computer system**

- (1) means-
  - (i) a computer; or
  - (ii) 2 or more interconnected computers; or

- (iii) any communication links between computers or to remote terminals or another device; or
  - (iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals, or any other device, and
- (2) includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software or communication facilities and stored data.

[599] Further, in the recent decision of *Dixon v R*<sup>178</sup> our Supreme Court found that “property”, in the context of s 249(1)(a), included digital files of CCTV footage.

[600] The provisions of s 101B(1)(c) are satisfied in that:

Para (i) the offences under s 249 are both punishable by sentences of imprisonment of more than 4 years.

Para (ii) Article 2(a) of TOC defines “organised criminal group” to mean:

... a *structured group* of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more *serious crimes* or offences established in accordance with this Convention, in order to obtain, *directly or indirectly, a financial or other material benefit*.

[601] The Request alleges the existence of “an organised criminal group”.

[602] The respondent group is greater than 3 people as the allegations are against 7 persons who were officers in the Mega businesses, 4 of whom are the respondents in this eligibility hearing.

[603] Article 2(c) of TOC defines a “structured group” to be:

... a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

---

<sup>178</sup> [2015] NZSC 147.

The allegation is that the Mega business was a structured group with the respondents each performing assigned roles within the business and not “randomly formed”.

[604] It is alleged that the members of the group shared the objective of committing a “serious crime” as defined in Art 2(b) of TOC to mean:

... conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty.

The aim of committing the serious crime was to obtain “directly or indirectly, a financial or other material benefit”. It is alleged that the popularity of the infringing content on Mega websites caused the receipt of some US\$25 million in advertising revenue and US\$150 million in premium subscription fees.

[605] All four respondents are in New Zealand.

[606] There is evidence to support the elements of the offences under s 249, that:

- (1) The respondents directly or indirectly accessed a computer system.
- (2) They obtained a pecuniary advantage, benefit, or valuable consideration, or caused loss to any other person.
- (3) The obtaining or causing was done dishonestly, or by deception and without claim of right.

[607] It is not in dispute that:

- (i) Mega was an online cloud storage business using a complex server network computer system.
- (ii) The Mega sites were operated by a very powerful computer system capable of handling a very large traffic flow and shared a “back-end database” giving access to all files.

- (iii) The respondents were all senior officers of Mega. Mr Ortmann and Mr van der Kolk were responsible for the programming and technical design of the system. They were also involved in the running of the site, including interrogating the database, administering the rewards system, processing takedown notices and editing the front pages. Mr Dotcom oversaw the running of the computer system and the uses to which it was put. He frequently issued directions about the operations of the website to Mr Ortmann and Mr van der Kolk.
  
- (iv) Mr Batato controlled advertising work on the Mega sites.

[608] There is evidence to support:

- (1) Mr Dotcom and Mr Batato having indirect if not direct access to the Mega computer system.
- (2) The respondents accessed other computer systems, such as their acquisition of the YouTube videos.
- (3) They knowingly distributed copyright infringing material through their own computer system by accessing a user's computer system.
- (4) The Mega computer system was run with the dishonest purpose of attracting, storing and then obtaining income from the traffic of content subject to copyright.
- (5) They knew they had no claim of right to copyright protected content.
- (6) They trafficked the copyright protected content so as to obtain income from it.
- (7) They were aware that their activities would result in a financial loss to the copyright holder or, at the very least, prejudice their property rights.

- (8) Their business model amounted to an illegal conspiracy under art II.16 of the Treaty.

[609] The alleged conduct in count 2 correlates with the offences in both s 249(1) and s 249(2). There is sufficient evidence to base a prima facie case against the respondents under s 249(1) and s 249(2) of the Crimes Act 1961.

***Count 2: Section 228 Crimes Act 1961***

[610] This offence may be deemed an extradition offence under the Treaty pursuant to s 101B as described in paras [594] and [596] herein.

[611] Section 228(1) says:

**228 Dishonestly taking or using document**

- (1) Every one is liable to imprisonment for a term not exceeding 7 years who, with intent to obtain any property, service, pecuniary advantage, or valuable consideration,—
- (a) dishonestly and without claim of right, takes or obtains any document; or
  - (b) dishonestly and without claim of right, uses or attempts to use any document

[612] The elements of the offence under s 228(b) are:

- (i) A use or attempted use of a document;
- (ii) It was done so with the intent to obtain a pecuniary advantage or valuable consideration; and
- (iii) It was done dishonestly and without claim of right.

[613] There is evidence to support the inference that the respondents conspired with the objective of obtaining digital file content, including copyright protected content, in the form of digital files and to make use of those files for the purpose of their own financial gain. Digital files are “documents” pursuant to s 217 of the Crimes Act.

[614] There is evidence to support the inference that they knew that many of the digital files they obtained contained copyright protected content, but they continued to use it for their own financial reward.

[615] The respondents are therefore eligible for surrender under the Act under s 228(b) due to the correlation of that section with the conduct alleged in count 2.

***Count 2: Section 131 Copyright Act 1994***

[616] Section 131 Copyright Act 1994 says:

**131 Criminal liability for making or dealing with infringing objects**

- (1) Every person commits an offence against this section who, other than pursuant to a copyright licence,—
- (a) makes for sale or hire; or
  - (b) imports into New Zealand otherwise than for that person's private and domestic use; or
  - (c) possesses in the course of a business with a view to committing any act infringing the copyright; or
  - (d) in the course of a business,—
    - (i) offers or exposes for sale or hire; or
    - (ii) exhibits in public; or
    - (iii) distributes; or
  - (e) in the course of a business or otherwise, sells or lets for hire; or
  - (f) distributes otherwise than in the course of a business to such an extent as to affect prejudicially the copyright owner—
- an object that is, and that the person knows is, an infringing copy of a copyright work.
- (2) Every person commits an offence against this section who—
- (a) makes an object specifically designed or adapted for making copies of a particular copyright work; or
  - (b) has such an object in that person's possession,—
- knowing that the object is to be used to make infringing copies for sale or hire or for use in the course of a business.
- (3) Subject to subsection (4), every person commits an offence against this section who—
- (a) causes a literary, dramatic, or musical work to be performed, where that performance infringes copyright in that work; or



- (b) causes a sound recording or film to be played in public or shown in public, where that playing or showing infringes copyright in that sound recording or film,—

knowing that copyright in the work or, as the case requires, the sound recording or film would be infringed by that performance or, as the case requires, that playing or that showing.

- (4) Nothing in subsection (3) applies in respect of infringement of copyright by the reception of a communication work.
- (5) Every person who commits an offence against this section is liable on conviction—
  - (a) in the case of an offence against subsection (1), to a fine not exceeding \$10,000 for every infringing copy to which the offence relates, but not exceeding \$150,000 in respect of the same transaction, or to imprisonment for a term not exceeding 5 years:
  - (b) in the case of an offence against subsection (2) or subsection (3), to a fine not exceeding \$150,000 or to imprisonment for a term not exceeding 5 years.

[617] The evidence in the ROC supports the conduct alleged in count 2. The same alleged conduct translates to breaches of s 131(1)(c) and of s 131(1)(d)(ii) or (iii).

[618] For s 131(1)(c), the evidence supports:

- (1) The respondents possessed objects (digital files);
- (2) The objects included infringing files of a copyright work;
- (3) The respondents knew those objects were infringing copies of a copyright work;
- (4) They were possessed with a view to committing an act infringing the copyright.
- (5) They did not possess the objects pursuant to any copyright licence; and
- (6) They possessed the objects in the course of a business.

[619] For s 131(1)(d)(ii) or (iii) there is evidence that:

- (1) The respondents exhibited in public the objects (digital files) or distributed the objects;
- (2) The objects included infringing files of a copyright work;
- (3) The respondents knew those objects were infringing copies of a copyright work;
- (4) The respondents did so other than pursuant to a copyright licence; and
- (5) They did so in the course of a business.

[620] The respondents are not able to hide behind a corporate shield. Section 133 of the Copyright Act says:

**133 Liability of officers of body corporate**

Where any body corporate is convicted of an offence against [section 131](#), every director and every person concerned in the management of the body corporate shall be guilty of the offence if it is proved—

- (a) that the act that constituted the offence took place with his or her authority, permission, or consent; and
- (b) that he or she—
  - (i) knew, or could reasonably be expected to have known, that the offence was to be or was being committed; and
  - (ii) failed to take all reasonable steps to prevent or stop it.

[621] Section 2(i) of the Copyright Act defines an “Internet service provider” (ISP) as follows:

**Internet service provider** means a person who does either or both of the following things:

- (1) offers the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing;
- (2) hosts material on websites or other electronic retrieval systems that can be accessed by a user

The evidence would support the conclusion that the Mega business is an ISP.

[622] The Copyright Act does exempt ISPs from some civil or criminal liability pursuant to s 92B, which says:

**92B Internet service provider liability if user infringes copyright**

- (i) This section applies if a person (A) infringes the copyright in a work by using 1 or more of the Internet services of an Internet service provider to do a restricted act without the consent of the copyright owner.
- (ii) Merely because A uses the Internet services of the Internet service provider in infringing the copyright, the Internet service provider, without more,—
  - (a) does not infringe the copyright in the work:
  - (b) must not be taken to have authorised A’s infringement of copyright in the work:
  - (c) subject to subsection (3), must not be subject to any civil remedy or criminal sanction.
- (2A) An Internet service provider does not infringe the copyright in the work, or authorise A’s infringement of the copyright in the work, merely because the Internet service provider knows of the infringement from information received as a result of anything done under sections 122A to 122U, provided that, in relation to the alleged infringement, the Internet service provider complies with all its obligations under those sections and under any regulations made under section 234(eb) to (eh).
- (3) However, nothing in this section limits the right of the copyright owner to injunctive relief in relation to A’s infringement or any infringement by the Internet service provider.
- (4) In subsections (1) and (2), **Internet services** means the services referred to in the definition of Internet service provider in section 2(1).

[623] A critical part of s 92B is that portion of subs (2) where the words “without more” appear. It is critical because s 92B, although providing exemptions from liability, does still contemplate the possibility of liability. That becomes apparent when s 92C is examined.

[624] Section 92C says:

**92C Internet service provider liability for storing infringing material**

- (1) This section applies if—
  - (a) an Internet service provider stores material provided by a user of the service; and

- (b) the material infringes copyright in a work (other than as a result of any modification by the Internet service provider).
- (2) The Internet service provider does not infringe copyright in the work by storing the material unless—
- (a) the Internet service provider—
    - (i) knows or has reason to believe that the material infringes copyright in the work; and
    - (ii) does not, as soon as possible after becoming aware of the infringing material, delete the material or prevent access to it; or
  - (b) the user of the service who provided the material is acting on behalf of, or at the direction of, the Internet service provider.
- (3) A court, in determining whether, for the purposes of subsection (2), an Internet service provider knows or has reason to believe that material infringes copyright in a work, must take account of all relevant matters, including whether the Internet service provider has received a notice of infringement in relation to the infringement.
- (4) An Internet service provider who deletes a user’s material or prevents access to it because the Internet service provider knows or has reason to believe that it infringes copyright in a work must, as soon as possible, give notice to the user that the material has been deleted or access to it prevented.
- (5) Nothing in this section limits the right of the copyright owner to injunctive relief in relation to a user’s infringement or any infringement by the Internet service provider.

[625] There is evidence before this Court to the effect that the respondents knew they were storing infringing material (s 92C(2)(a)(i)) and that they failed to delete or prevent access to that material as soon as possible after they became aware of it (s 92C(2)(a)(ii)). There is evidence that the respondents failed to delete infringing files as soon as possible, usually only deleting the URL providing the linkage to the file but leaving in existence many other URLs linking to the infringing file, thereby not preventing access to it. There is evidence that they frequently led a copyright owner to believe that a file had been deleted when only one URL had been deleted. There is evidence that the respondents’ claim that the other URL link would or might have the copyright owner’s authority to retain the remaining URL links was self-serving and disingenuous.

[626] The purpose and intent of s 92B is to provide a “safe harbour” for ISPs that unintentionally have their storage used by others to store illegitimate materials, a true “dumb pipe”. By way of example in other contexts, a publisher of a book, a DVD or a movie should not be held responsible for any illegitimate use other persons might make of that book, DVD or movie. Section 92B protects them from any such innocent involvement.

[627] Protection under s 92B is not available on the evidence adduced at this hearing. There is evidence before the Court sufficient to establish that the respondents were in the course of a business that knowingly uploaded copies of copyright protected material, they kept it with a view to committing acts that would infringe the copyright, they were complicit in promulgating that they possessed such material, and distributed it to large numbers of people for their own financial gain. The conduct alleged in count 2 therefore translates to a deemed extradition offence under both s 131(1)(c) and s 131(1)(d)(ii) or (iii).

***Count 3: Conspiring to Launder Money***

[628] In count 3 it is alleged that the respondents conspired to launder the monetary proceeds from Mega’s unlawful business activities knowing that the money was unlawfully obtained. This money was then distributed in a number of ways. Some of this money was reinvested in the business; some of it was paid to the respondents as drawings or salaries.

[629] The applicant submits that count 3 corresponds to the extradition offence described in Art II.19 as:

19. Receiving and transporting any money, ... or other property knowing the same to have been unlawfully obtained.

[630] The Treaty offence consists of the following elements:

- (1) The respondents received money;
- (2) The respondents transported that money; and

- (3) The respondents knew the money had been unlawfully obtained.

The conduct alleged for count 3 also includes the allegation that the respondents conspired to so launder the money.

[631] It is not disputed that the respondents received money from the Mega businesses, or that money was transported from users to Mega and then on to the respondents. There is also sufficient evidence to find a prima facie case has been established that the respondents knew that at least some of the funds they received from the Mega businesses came from the traffic of infringing copyright material. The respondents are therefore eligible for surrender on count 3 under Art II.19 of the Treaty.

***Count 1: Conspiracy to Commit Racketeering***

[632] The conduct alleged in this count involves the commission of offences by the respondents, as conspirators, carried out as part of the unlawful activities of a criminal enterprise formed by the respondents for the purpose of enrichment. The applicant submits that this conduct corresponds with the offence of participation in an organised criminal group under s 98A of the Crimes Act 1961, which s 101B(1)(a) of the Extradition Act expressly deems to be a Treaty offence.

[633] The applicant submits that the specific acts comprising the racketeering activities in count 1, namely criminal copyright infringement, laundering and wire fraud, also correspond as Treaty offences themselves. Section 101B of the Act deems s 98A Crimes Act to be an extradition offence.

[634] The conduct alleged in count 1 is that:

- (1) The respondents formed an enterprise;
- (2) They agreed to run the enterprise to commit multiple acts of indictable crime (criminal copyright infringement, laundering, and wire fraud);
- (3) For the purposes of enriching themselves.

[635] The New Zealand offence pursuant to s 98A of the Copyright Act has the additional requirements:

- (1) Knowledge of the group's objectives; and
- (2) Knowledge or recklessness that their participation contributes to the occurrence of criminal activity which thereby contributes to the objectives.

[636] Section 98A Crimes Act says:

**98A Participation in organised criminal group**

- (1) Every person commits an offence and is liable to imprisonment for a term not exceeding 10 years who participates in an organised criminal group—
  - (a) knowing that 3 or more people share any 1 or more of the objectives (the particular objective or particular objectives) described in paragraphs (a) to (d) of subsection (2) (whether or not the person himself or herself shares the particular objective or particular objectives); and
  - (b) either knowing that his or her conduct contributes, or being reckless as to whether his or her conduct may contribute, to the occurrence of any criminal activity; and
  - (c) either knowing that the criminal activity contributes, or being reckless as to whether the criminal activity may contribute, to achieving the particular objective or particular objectives of the organised criminal group.
- (2) For the purposes of this Act, a group is an organised criminal group if it is a group of 3 or more people who have as their objective or one of their objectives—
  - (a) obtaining material benefits from the commission of offences that are punishable by imprisonment for a term of 4 years or more; or
  - (b) obtaining material benefits from conduct outside New Zealand that, if it occurred in New Zealand, would constitute the commission of offences that are punishable by imprisonment for a term of 4 years or more; or
  - (c) the commission of serious violent offences; or
  - (d) conduct outside New Zealand that, if it occurred in New Zealand, would constitute the commission of serious violent offences.
- (3) A group of people is capable of being an organised criminal group for the purposes of this Act whether or not—
  - (a) some of them are subordinates or employees of others; or

- (b) only some of the people involved in it at a particular time are involved in the planning, arrangement, or execution at that time of any particular action, activity, or transaction; or
- (c) its membership changes from time to time

[637] It is not in dispute that the respondents were officers of the Mega businesses. Those businesses, the applicant alleges, are an organised criminal group due to at least part of its activities involving multiple acts of criminal copyright infringement, wire fraud, and subsequent money laundering of the profits obtained from these activities. Knowledge of the alleged criminal activities can be inferred from the participation by each of the respondents' active involvement in the running of the business and promotion of its growth.

[638] All the elements of the offence in s 98A have been satisfied to a prima facie standard by the applicant and the respondents are therefore eligible for surrender on count 1.

#### **Counts 4-8: Discrete Acts of Copyright Infringement**

[639] Counts 4 to 8 each allege specific acts of copyright infringement with all the respondents named in each count. Count 4 relates to the uploading of the movie "Taken"; counts 5 to 7 relate to the alleged distribution of copyright works for financial gain over specified periods of time. Count 8 relates to the distribution of YouTube videos over a specific time period.

[640] For each of counts 4 to 8 it is alleged that the offending has been through Megaupload.com and Megavideo. It is alleged that the distribution of copyright infringing files is a manifestation of the conspiracy in action between the respondents. It is said that they intended Mega to operate as a vehicle for copyright infringement, that they participated in their corporate roles in that business knowing that multiple infringements would be a consequence, and did so for the purpose of financial gain to themselves. It is alleged that knowledge of specific infringements for each count can be inferred as Mr van der Kolk uploaded the copyright infringing file in count 4 and there were takedown notifications for copyright infringing files for counts 5 to 8, and those files remained publicly available on the Mega sites until this was closed down in January 2012.



[641] As described in paras [588] to [589] above, this same analysis places the alleged offending as falling within Art II.16 of the Treaty. It is alleged that the elements of Art II.16 are satisfied as the respondents conspired to run the Mega business in such a manner as to include and encourage the uploading and distribution of copyright infringing files, in that:

- (1) There was an obtaining of property (by the uploading of digital files subject to copyright).
- (2) The property was retained on the Mega servers.
- (3) The retention of the property on Mega servers was for the purpose of selling subscriptions for access to the files and to generate advertising revenue due to the large volume of traffic so generated.

[642] The conduct alleged in count 4 is that the respondents wilfully, for the purposes of commercial advantage and private financial gain, infringed copyright by distribution of a copyright work by making it available on a computer network accessible to members of the public.

[643] It is alleged that each of counts 4 to 8 is a furtherance of the copyright conspiracy in count 2. The correlating offences are in the Crimes Act, s 249(1), s 249(2), s 228(b), and in the Copyright Act, s 131(1)(c) and 131(1)(d)(ii) or (iii), and s 137. The same analysis applies as in count 2 in para [588] to [627] above, and the same conclusion is reached.

#### ***Count 4***

[644] On 28 October 2008, Mr van der Kolk is alleged to have uploaded to Mega a copy of the Copyrighted movie “Taken”. He emailed an URL link to another person the same day. It was downloaded at least 9 times through Megavideo.com and was viewed by FBI Agent Poston in November 2011. “Taken” was not to be released in the United States of America theatres until January 2009 and not to be commercially released until May 2009.

[645] It is alleged that there was private financial gain to the respondents as the movie was obtained without payment to the copyright owner and distributed to subscribers who wished to gain access to it. It was intended that the movie could be accessed through Mega and it was intended to earn income by virtue of that distribution. There was a loss to the copyright owner described in *Scott v Metropolitan Police Commissioner*.<sup>179</sup>

[646] There is evidence that the other respondents knew that Mr van der Kolk downloaded infringing files, and knew that the Mega site was used to make use of copyright infringing material as part of the Mega business. All respondents and Mega were therefore participating in the running of a business they knew to be breaching the copyright owner's rights.

[647] It is submitted for Mr van der Kolk that:

- (1) The count is based upon him sending a link to "Taken" on 25 October 2008.
- (2) "Taken" was not due for release in the USA until January 2009 and would not be commercially distributed until 12 May 2009.
- (3) As at 25 October 2008, "Taken" had been released to cinemas in 30 countries worldwide.
- (4) "Taken" was likely to have been distributed on DVD in at least eight countries prior to 25 October 2008.

[648] It is further submitted for Mr van der Kolk that there is no evidence that:

- (1) Neither Mr van der Kolk nor the recipient was located in the USA on 25 October 2008.

---

<sup>179</sup> *Scott v Metropolitan Police Commissioner* [1975] AC 819.

- (2) The file was uploaded by users in the USA prior to its release in that country.

[649] Whether “Taken” was commercially available in certain countries and when that occurred does not necessarily mean that the copyright owner of “Taken” did not have its property rights prejudiced. It could still be downloaded and distributed illegitimately in contravention of the copyright owner’s property rights. The applicant’s allegation is that although the initial uploading and distribution took place on 25 October 2008, it was a continuing course of action and “Taken” was still available on Mega until Mega was closed down in January 2012. It is the applicant’s case that what happened with the film “Taken” was a specific example of the respondents’ modus operandi.

[650] The evidence adduced by the applicant is sufficient to establish a prima facie case on each of the sections, and Art II.16 of the Treaty. The respondents are therefore eligible for extradition under count 4.

#### *Count 5*

[651] This alleged offending concerns acts of distribution of copyright infringing content for a 180 day period up to and including 19 January 2012. The alleged conduct translates into deemed Treaty offending under ss 249 and 228 Crimes Act, s 131 Copyright Act, and Art II.16 of the Treaty as in count 4.

[652] The elements of the alleged offending are the same as those set out in count 2.

[653] The applicant has adduced evidence of Mega having possession of a number of movies in breach of the property rights of the copyright owner. They have also adduced evidence of the scale usage of the copyright infringing material and the actions taken in response to takedown notices. These include:

- (1) Unique file of “Lord of the Rings”:
  1. More than 100 URL links to this infringing file;

2. 89 links still active and publicly available in 2012;
  3. Viewed at least 250 times;
  4. At least 4 links removed after takedown notification.
- (2) Two unique files embodying “Twilight Saga: Breaking Dawn – Part 1”:
1. In two files;
  2. The first file viewed at least 32,000 times from Mega sites;
  3. The second file viewed at least 18,000 times;
  4. At least 17 URL links to first file;
  5. 16 of those links still active in 2012;
  6. At least 12 links to the second file;
  7. 11 of those links still active in 2012;
  8. At least 1 link to each file removed for copyright infringement.
- (3) Unique file of “Happy Feet Two”:
1. Viewed more than 1,000 times;
  2. More than 100 URL links;
  3. 74 of those links still active in 2012;
  4. At least 4 links removed after takedown notifications.
- (4) Unique file of “Puss in Boots”:

1. Viewed at least 10,000 times;
  2. More than 150 URL links;
  3. More than 119 of those links still active in 2012;
  4. At least 14 URL links removed for takedown notification.
- (5) Unique file of “Bored to Death” episode:
1. Viewed at least 1,800 times;
  2. More than 145 URL links;
  3. 136 of those links still active in 2012;
  4. At least 3 links removed for takedown notification;
  5. Abuse tool and email notification of infringement. 20 new links created after email notification in November 2011, resulting in 6 further views.
- (6) Unique file of “Dungeon Siege III” (software)
1. More than 45 URL links;
  2. 34 of those links still active in 2012;
  3. 7 URL links removed after takedown notification.

[654] Some of the unique files have had links disabled for copyright infringement, but the file and other links have been retained so that access to the copyright infringing content could and did continue. It is submitted that this is indicative of a course of behaviour from which a dishonest interest can be inferred. The action of removing a link to mollify a copyright owner but keeping the file with, in some cases

many, links to it did little to abate the loss to a copyright owner and enabled the Mega business to continue to profit from the copyright infringing content.

[655] There is sufficient evidence to establish a prima facie case pursuant to s 228 Copyright Act that there was a dishonest use of documents (in the form of copyright infringing digital files) that resulted in the respondents obtaining a pecuniary advantage. There is also sufficient evidence to establish a prima facie case pursuant to s 131 Copyright Act that there was a distribution of copyright infringing objects and the respondents knew the Mega business was being run as a vehicle to distribute the copyright infringing files. A prima facie case is therefore established under count 5 so as to render the respondents eligible for extradition.

### *Count 6*

[656] This alleged offending concerns acts of distribution of copyright infringing content for a 180 day period up to and including 31 August 2010. The alleged conduct in count 6 translates into deemed Treaty offences under ss 249 and 228 Crimes Act, s 131 Copyright Act, and Art II.16 of the Treaty as in count 5. The same elements of the offences alleged to be established also apply. The only remaining issue for count 6 is whether the evidence is sufficient to find that a prima facie case has been established.

[657] The applicant has adduced evidence that:

- (i) A particular copyright infringing file with a single, unique MD5 hash embodying a motion picture “IP Man 2:”
  1. Was downloaded at least 750,000 and viewed at least 50,000 times from Mega sites;
  2. Had more than 200 Mega URL links pointing to it;
  3. 168 of those links were still active and publicly available in January 2012;

4. 3 of the 200 links were removed after receipt of copyright infringement notification.
- (ii) Two particular copyright infringing files with a single, unique MD5 hash (Parts One and Two) embodying a motion picture “Prince of Persia:”
1. Part One was downloaded at least 110,000 and Part Two was downloaded at least 260,000 times;
  2. Part One had at least 22 Mega URL links pointing to it;
  3. At least 13 of those links were still active and publicly available in January 2012;
  4. Part Two had at least 16 Mega URL links pointing to it;
  5. Eight of those links were still active and publicly available in January 2012;
  6. Mega removed at least one URL links for each part after receipt of copyright infringement notification.
- (iii) A particular copyright infringing file with a single, unique MD5 hash embodying a motion picture “Alice in Wonderland.”
1. Was downloaded at least 260,000 times;
  2. Had more than 190 Mega URL links pointing to it;
  3. 129 of those links were still active and publicly available on the Mega sites in January 2012;
  4. Mega removed at least 35 links after infringement notification by the copyright owner. Email notifications were made by APCM in April 2010, but 10 new links to this file were created after that

date and these resulted in 110 downloads and 6,000 views of the file.

- (iv) A particular copyright infringing file with a single, unique MD5 hash embodying a motion picture “Percy Jackson & the Olympians: The Lightning Thief:”
1. Was downloaded at least 230,000 times from Mega sites;
  2. More than 40 Mega URL links pointing to this file;
  3. 29 of those links were still active in January 2012;
  4. At least 9 links were removed after notification by the copyright owner. These included 8 separate email notifications by 20<sup>th</sup> Century Fox in March/May 2010. After March 2010, more than 25 new URL links to this file were created and publicly distributed and these resulted in at least 190,000 downloads and 5,000 views.

[658] The same conclusion can therefore be reached as in paragraph [626] herein that the respondents are eligible for extradition in count 6.

### *Count 7*

[659] This alleged offending concerns acts of distribution of copyright infringing content for a period of 180 days up to and including 16 August 2008. The same Treaty offences apply as in count 6 (see para [560]) and the only remaining issue for count 7 is to decide if a prima facie has been established.

[660] The applicant has adduced evidence that:

- (i) “Cloverfield” (motion picture), downloaded up to 506,535 times;
- (ii) “Meet the Spartans” (motion picture) downloaded up to 144,174 times;



- (iii) “The Forbidden Kingdom” (motion picture) downloaded tens of thousands of times;
- (iv) An episode of “Prison Break” (television programme) downloaded tens of thousands of times.

[661] In particular:

- (i) Two particular copyright infringing files, each with a single unique MD5 hash (Parts One and Two) embodying “The Forbidden Kingdom”:
  - 1. Part One downloaded at least 99,000 times from the Mega sites;
  - 2. Part Two downloaded at least 97,000 times;
  - 3. At least 6 URL links pointed to Part One;
  - 4. At least 3 of those links were still active and publicly available in January 2012;
  - 5. At least 7 URL links pointed to Part Two;
  - 6. At least 4 of those links were still active and publicly available in January 2012.
  - 7. Mega removed at least one link for each part of the movie after infringement notification by the copyright owner.
- (ii) A particular copyright infringing file with a single, unique MD5 hash embodying an episode of the television series “Prison Break”:
  - 1. Was viewed at least 94,000 times and viewed at least 500 times from Mega sites.
  - 2. More than 55 Mega URL links pointed to this file;

3. 48 of those links were still active and publicly available on Mega sites in January 2012;
  4. At least 8 links were removed after infringement notification by or on behalf of the copyright owner.
- (ii) A particular copyright infringing file with a single, unique MD5 hash embodying an episode of the motion picture “Hancock”:
1. Was downloaded at least 160,000 times and viewed at least 530 times from Mega sites;
  2. More than 200 Mega URLs linked to this file;
  3. 164 of those links were still active and publicly available on Mega sites in January 2012;
  4. At least 30 of the URL links were removed after infringement notification by or on behalf of the copyright owner, including two emails dated 9 August 2008;
  5. After that date, more than 150 new Mega URL links were created, through which 4,000 downloads and 170,000 views occurred.

[662] On 20 August 2003 s 131A of the Copyright Act came into force. It says:

Despite s 14 of the Summary Proceedings Act 1957, an information in respect of an offence against s 131 may be laid at any time within 3 years of the time when the matter of the information arose.

It was then repealed on 1 July 2013.

[663] The offences alleged in count 7 are within a period when s 131A was in force. Under s 24(2)(d) of the Act this Court must be satisfied that the evidence produced would, according to the law of New Zealand, justify a person’s trial if the offence

had occurred within the jurisdiction of New Zealand. On that basis, the respondents would not be eligible for surrender based on s 131.

[664] Section 11 of the Act says that the provision of this Act must be construed to give effect to the Treaty. The applicant submits that a domestic time limit is not a bar to determining eligibility for a Treaty offence and it was a continuous offence up until January 2012.

[665] With respect to the applicant's submission, I do not agree. Section 131A is quite specific and does not allow for any exceptions. It is clear that the alleged offending in count 7 is not within the jurisdiction of this Court under s 131 according to the law of New Zealand. Count 7 is also framed for a specific period up to the end including 16 August 2008. It does not lay a charge of continuous offending after that date. The respondents are therefore not eligible for surrender on count 7 pursuant to s 131.

[666] The evidence produced at this hearing does establish a prima facie case for count 7 pursuant to ss 249 and 228 of the Crimes Act and pursuant to Art II.16 of the Treaty so as to render the respondents eligible for extradition.

### *Count 8*

[667] In count 8, the US grand jury charges that the respondents for the 180 days up to and including 31 October 2007, in the Eastern District of Virginia and elsewhere, wilfully infringed copyrights, for the purposes of commercial advantage and private financial gain, from the YouTube.com platform, by reproducing and distributing by electronic means during the 180-day period at least 10 copies and phonorecords of one or more copyrighted works which had a total retail value in excess of US\$2,500.

[668] The alleged conduct translates into the same deemed Treaty offences as count 2 herein. The remaining issue for count 8 is whether the applicant's evidence establishes a prima facie case.

[669] The applicant alleges a mass acquisition of YouTube videos in 2007. The ROC provides evidence that at least 10 copies of copyright infringing material were

reproduced and distributed by a Mega site. It also provides evidence of at least 10 YouTube videos from 2007 were still available on Mega sites in January 2012 and the YouTube videos had been viewed thousands of times. There is also evidence that when the copyright owners of those clips discovered them on Mega sites and complained that they were deceived about the action taken in response to the complaint. There is also evidence that the uploading of the copyright infringing material was performed or directed by at least 3 of the respondents in this hearing.

[670] For the same reasons given in paragraphs [633] to [636] count 8 must fail with respect to the charge pursuant to s 131 of the Copyright Act. However, the evidence does establish a prima facie case for count 8 pursuant to ss 249 and 228 of the Crimes Act and pursuant to Art II.16 of the Treaty so as to render the respondents eligible for extradition.

***Counts 9-13: Fraud by Wire and Aiding and Abetting Fraud by Wire***

[671] Counts 9-13 allege conduct of fraud by wire, and aiding and abetting fraud by wire. They relate to particular occasions when Mega email accounts were used to send messages to copyright owners that are alleged to be deceptive. The evidence in the ROC alleges a plan to deceive copyright owners by:

- (i) Encouraging them to believe that files would be removed from Mega servers when infringing content had been identified when, in reality, only the link specified by the copyright owner, and by which the infringing file was detected, was deleted.
- (ii) Encouraging them to believe that repeat infringers would have their user access terminated.
- (iii) Encouraging them to believe that the operation of the Abuse Tool would result in content or files being deleted, when in fact only specific links were removed by the Tool.
- (iv) Encouraging them to believe that Mega was taking active steps to curb or prevent copyright infringement.

- (v) Maintaining a façade of Mega’s compliance with obligations imposed by copyright laws.

[672] The alleged conduct translates into a Treaty offence under Art II.16. It would amount to a joint enterprise to defraud copyright owners by deceiving them into believing that the Mega business was taking active steps to prevent copyright infringement. Such deception would allow the respondents to continue to profit from the use of that copyright content. For essentially the same reasons the alleged specific acts of fraud are captured by s 249 and s 228(b) Crimes Act as set out in the earlier counts.

[673] The applicant submits that the alleged conduct also translates into a Treaty offence pursuant to s 240 Crimes Act, which says:

**240 Obtaining by deception or causing loss by deception**

- (1) Every one is guilty of obtaining by deception or causing loss by deception who, by any deception and without claim of right,—
  - (a) obtains ownership or possession of, or control over, any property, or any privilege, service, pecuniary advantage, benefit, or valuable consideration, directly or indirectly; or
  - ...
  - (d) causes loss to any other person.

Deception is defined in subsection (2) to mean:

- (a) a false representation, whether oral, documentary, or by conduct, where the person making the representation intends to deceive any other person and—
  - (i) knows that it is false in a material particular; or
  - ...
- (c) a fraudulent device, trick, or stratagem used with intent to deceive any person.

[674] It is submitted by the applicant that the alleged conduct in counts 9-13 involved:

- (1) Knowingly created and sent false communications intended to deceive the recipients;
- (2) By virtue of the false messages the respondents obtained (by retaining) property (digital files subject to property rights);
- (3) They obtained directly or indirectly pecuniary advantages and benefits from the retention and continued use of the property.

The alleged conduct satisfies the elements of an offence under 240 and qualifies as a deemed Treaty offence.

[675] The alleged conduct for each of counts 9 to 13 is set out below, citing the appropriate paragraph numbers from the ROC:

Paragraph [34i]:

On or about November 23, 2010, members of the Mega Conspiracy caused a communication to be sent from a computer server in the Eastern District of Virginia to a representative of a copyright holder stating “1 file and 1 video removed from our system” in response to a takedown request that included a link to the 2010 version of the copyrighted film “A Nightmare on Elm Street.” This representation was false because the Mega Conspiracy only disabled the specific URL link identified, and failed to disable access to the underlying copyright-infringing material or remove the file from the server.

Paragraph [96e]:

With respect to Paragraphs 34(1) of the Record of the Case, the November 23, 2010 communication was an automated online response, generated pursuant to software coding written by a member(s) of the Mega Conspiracy, in response to a takedown request that included a link to the 2010 version of the copyrighted film “A Nightmare on Elm Street.” Warner is the copyright owner.

### ***Count 10***

Paragraph [34j]:

On or about March 9, 2011, members of the Mega Conspiracy caused a communication to be sent from a computer server in the Eastern District of

Virginia to a representative of a copyright holder stating “2 files removed from our system” in response to a takedown request that included a link to the 2009 version of the copyrighted film “Friday the 13th” (in two parts). This representation was false because the Mega Conspiracy only disabled the specific URL link identified, and failed to disable access to the underlying copyright-infringing material or remove the file from the server.

Paragraph [96f]:

With respect to Paragraphs 34(j) of the Record of the Case, the March 9, 2011 communication was an automated online response, generated pursuant to software coding written by a member(s) of the Mega Conspiracy, in response to a takedown request that included a link to the 2009 version of the copyrighted film “Friday the 13th” (in two parts). Warner is the copyright owner.

### ***Count 11***

Paragraph [34k]:

On or about March 11, 2011, members of the Mega Conspiracy caused a communication to be sent from a computer server in the Eastern District of Virginia to a representative of a copyright holder stating “2 files removed from our system” in response to a takedown request that included links to copies of the copyrighted television show “Modern Family”. This representation was false because the Mega Conspiracy only disabled the specific URL links identified, and failed to disable access to the underlying copyright-infringing material or remove the file from the server.

Paragraph [96g]:

With respect to Paragraphs 34(k) of the Record of the Case, the March 11, 2011 communication was an automated online response, generated pursuant to software coding written by a member(s) of the Mega Conspiracy, in response to a takedown request that included links to copies of the copyrighted television show “Modern Family”. Fox is the copyright owner.

### ***Count 12***

Paragraph [34l]:

On or about April 30, 2011, members of the Mega Conspiracy caused a communication to be sent from a computer server in the Eastern District of Virginia to a representative of a copyright holder in response to a takedown request that included a link to the copyrighted motion picture “Fast Five”. This representation was false because the Mega Conspiracy only disabled the specific URL link identified, and failed to disable access to the underlying copyright-infringing material or remove the file from the server.

Paragraph [96h]:

With respect to Paragraph 34(l) of the Record of the Case, the April 30, 2011 communication was an automated online response, generated pursuant to software coding written by a member(s) of the Mega Conspiracy, in response to a takedown request that included a link to the copyrighted motion picture “Fast Five”. NBC Universal is the copyright owner.

Paragraph [137b]:

As described in Paragraphs 34(l) and 96(h) of the Record of the Case, on or about April 30, 2011, members of the Mega Conspiracy caused a communication to be sent from a computer server in the Eastern District of Virginia to a representative of a copyright holder in response to a takedown request that included a link to the copyrighted motion picture “Fast Five”. NBC Universal is the copyright owner. The representation was an automated online response indicating that a certain number of “file[s]” and “video[s]” were removed from the system, and the representation was generated pursuant to software coding written by a member(s) of the Mega Conspiracy. The representation was false because the Mega Conspiracy only disabled the specific URL link identified and failed to disable access to the underlying copyright-infringing material or remove the file from the server.

***Count 13***

Paragraph [34n]:

On or about August 10, 2011, members of the Mega Conspiracy caused a communication to be sent from a computer server in the Eastern District of Virginia to a representative of a copyright holder stating “6 files and 6 videos removed from our system” in response to a takedown request that included links to the 2010 version of the copyrighted motion picture “A Nightmare on Elm Street”. This representation was false because the Mega Conspiracy only disabled the specific URL links identified, and failed to disable access to the underlying copyright-infringing material or remove the file from the server.

Paragraph [96i]:

With respect to Paragraph 34(n) of the Record of the Case, the August 10, 2011 communication was an automated online response, generated pursuant to software coding written by a member(s) of the Mega Conspiracy, in response to a takedown request that included links to the 2010 version of the copyrighted motion picture “A Nightmare on Elm Street”. Warner is the copyright owner.

[676] The alleged deception of the affected copyright owners – Warner, Fox and NBC Universal – is contained in paragraphs [83], [85] and [95] of SROC 1.



[677] The alleged conduct in counts 9 to 13 is sufficient to establish a prima facie case against the respondents. The respondents are therefore eligible for extradition under counts 9 to 13.

### **Respondents' Opposition**

[678] The applicant has established a prima facie case for each count in the superseding indictment. The respondents are entitled to challenge the applicant's case and do so. Those challenges are considered below.

#### ***Mega's Terms and Conditions of Use***

[679] For the first respondent it is submitted that the Mega businesses had terms and conditions of use to specifically prohibit the uploading of unauthorised content which expressly include content protected by copyright.

[680] The applicant has not disputed the existence of these policies. The applicant's case is built upon the alleged conduct of the respondents, not upon the existence of the policies. The respondents may wish to raise the existence of these policies as an indication of the respondents' intent not to breach copyright owners' proprietary rights, but that is a competing argument which is an issue for trial, not this Court.

#### ***Mega's Takedown Policy***

[681] The first respondent submits that Mega's terms and conditions also specifically refer to a "takedown" mechanism for copyright holders to complain of abuse. Further they say Mega was receiving tens of thousands of such notices per day and responding to them in accordance with that policy. They also submit that Mega offered verified copyright holders a "Direct Delete" access to allow copyright holders to delete infringing files. They also submit that the home pages of the Mega sites did not have a search tool where a user could search all content stored on the sites, which they say minimised copyright infringement. Also, they submit, Mega knew of "linking sites" where URLs of content uploaded to Mega would be posted, in the same way as any ISP. They say that Mega had no control over these sites, it

refused to pay for traffic to Mega from those sites and was not in a position to determine if the content was copyright infringing.

[682] The applicant's case is built upon the alleged conduct of Mega and the respondents as officers of that business. The applicant's case is not based on the stated policies of Mega or the takedown mechanism it might have in place. Once again, the respondents might wish to raise these matters at trial as evidence of their good intent, but that is a competing argument to the applicant's case and should be dealt with at trial. It does not detract from or undermine the applicant's case.

### ***Rewards Programme***

[683] The first respondent submits that it did run a rewards programme for premium account holders but the terms and conditions required uploaders to honour copyright. For the same reasons given above, this is also a trial issue.

### ***Duty of Candour and Good Faith***

[684] It is for the requesting state to decide what material it will rely upon at the eligibility hearing. That is, however, subject to its duty of candour and good faith. The requesting state has a duty to disclose evidence which renders worthless, undermines or seriously detracts from the evidence upon which the requesting state has placed reliance: *Dotcom v USA*.<sup>180</sup> Our Supreme Court says:

[153] ... The requesting state has the right to decide what evidential material it wishes to rely on and put before the District Court in a record of the case against the requested person. The state is not required to put forward all information that it wishes to rely on at trial or to provide in the record of the case copies of all documents and exhibits summarised therein. ... The requesting state must, however, satisfy the Court that it has put forward sufficient evidence to meet the prima facie case standard and, in doing so, must comply with its obligations of candour to the extradition court.

[685] The Supreme Court went on to say:

[190] A person the subject of extradition proceedings in New Zealand is not entitled to disclosure of the kind available in domestic criminal proceedings. The entitlement is no more than to receive, in advance

---

<sup>180</sup> *Dotcom v USA* [2014] 1 NZLR 355 at para [152].

of the extradition hearing, the material that the requesting state will rely on before the extradition court. Where a requesting country has exempted status, the case brought against a requested person may be presented through the record of case procedure. Where the record of case process is used, the evidence may be presented in summary form rather than fully recited and it is not mandatory to include all the documents and exhibits relied on by the requesting state. The certification provisions in s 25 mean that, in general, reliance of the evidence presented by the requesting state is presumed, although that is rebuttable.

[686] The first respondents submit that the applicant is in breach of its duty of candour and good faith by:

- (i) Asserting that a doctrine of secondary criminal copyright infringement exists in the USA;
- (ii) Refusing to disclose its case;
- (iii) Failing to preserve evidence for trial;
- (iv) Loss of users' data;
- (v) Frustrating access to personal and official information;
- (vi) Presenting an unreliable ROC;
- (vii) Providing incorrect translations;
- (viii) Failing to provide context of communications relied upon;
- (ix) Basing its case on inferences rather than facts;

[687] In addition, the second and third respondents further submit:

- (x) The Court has been misled by the applicant in critical technical areas as to the operation of the internet in general and cloud storage facilities in particular;

- (xi) Misled the Court as to the copyright status of the motion picture “Taken”;
- (xii) Misled the North Shore District Court in relation to obtaining ex parte provisional arrest warrants;
- (xiii) The applicant has through its counsel attempted to mislead this Court as to the proper application of the doctrine of transposition in this case;
- (xiv) Failed to discuss that this case against the respondents is a “test case” as far as US law is concerned, and there is no basis for certifying that the evidence in the ROC justifies prosecution in the USA.

[688] Each of these submissions are considered next using the same paragraph numbers:

- (i) Section 25(3)b) of the Act says a ROC is admissible as evidence if certified pursuant to subs (3A). Mr Jay Prabhu as Assistant United States Attorney prosecuting this case has provided this certificate. The first respondent submits that Mr Prabhu in presenting the ROC is asserting a doctrine of secondary criminal copyright infringement exists in USA law. The first respondent has presented an affidavit from Professor Lessig of Harvard Law School who has a different view. Professor Lessig also expresses the view that the streaming of copyright material does not constitute a felony but a misdemeanour, and therefore cannot be the subject of an extradition request.

Both Mr Prabhu and Professor Lessig are well qualified to express their views but any disagreement upon the interpretation of US law is a matter for the US courts, not this Court. The ROC also alleges that illegal downloading of copyright material took place, not merely streaming. That issue also is a trial issue for consideration by the US court. Neither are eligibility hearing issues. A difference in expert

views does not amount to a breach of the duty of candour and good faith.

- (ii) This issue has already been considered. Nothing new has been advanced to change the conclusion already reached and does not amount to a breach of the duty of candour and good faith.
- (iii) It is submitted that in presenting its case through the ROC procedure it is required to be accompanied by an affidavit stating “that the evidence has been preserved for use in the person’s trial”: s 25(3)(a). An affidavit to this effect has been filed by Mr Prabhu.

The first respondent submits that since January 2012 the servers of the Mega group have been unplugged from a power source and therefore not running and not being maintained. The submission is that the data on the servers will corrupt over time and much of the data will have been lost to the respondents should they wish to access it to defend themselves at trial.

The obligation upon the applicant for this eligibility hearing is to provide the affidavit pursuant to s 25(3)(a) and that affidavit has been provided. That affidavit confirms that the applicant has preserved for use at trial all the evidence set out in the ROC. There is not a requirement that all data which might or might not be relevant for trial has been preserved. Should it be the case that the respondents require evidence from any data that is lost, then that is a fair trial issue for the US Court to consider. It is not an issue for this Court and does not constitute a breach of the duty of candour and good faith.

- (iv) This is covered in subpara (iii) above.
- (v) It is submitted that Mr Dotcom has made various requests for personal and official information under the Privacy and the Official Information Acts in New Zealand, and he has been frustrated in these efforts

through what is alleged to be unlawful withholding of information (in toto and by redaction) and the transfer of his requests to the Crown Law office. It is also alleged that the transfer of requests was a deliberate litigation strategy to deny access to evidence by Mr Dotcom. It is submitted that this conduct was performed on behalf of the applicant by counsel appearing for the applicant at this eligibility hearing, and a denial of evidence and a strategy of delay is inconsistent with the duty of candour and good faith.

The allegations concerning the actions of counsel for the applicant are very serious, but it is not the role of this Court to consider the alleged impropriety of the applicant's counsel. It is the role of this Court to consider whether the allegations are such that the respondents cannot have had a fair hearing at this eligibility hearing due to an alleged breach of candour and good faith.

This issue has already been substantially dealt with.

The first respondent submits that this is all relevant to the information collected through surveillance or interception, the circumstances behind the granting of residence in New Zealand to Mr Dotcom and his family, the basis for the raid on Mr Dotcom's house and whether this was done to obtain global attention for domestic political purposes in the USA, and to the seizure of assets and information.

The submissions for the first respondent are historical in that the alleged actions have taken place well prior to this eligibility hearing. Many of these allegations have already been dealt with in the New Zealand courts, or are still subject to ongoing litigation. But they are not relevant to the decision of this Court in deciding whether a prima facie case has been established for eligibility for extradition of the respondents. Ongoing and repetitive allegations of conduct previously rejected by the Courts or being appropriately dealt with in other litigation does not impact so as to cause this hearing to be unfair, and

does not establish a breach of the duty of candour and good faith in this hearing.

- (vi) The first respondent submits the ROC is unreliable because it does not clearly set out:
  - (a) All investigations undertaken by whom and when
  - (b) A full summary of all evidence obtained
  - (c) The identity and qualifications of proposed witnesses
  - (d) Full transcripts of skype communications
  - (e) How qualitative figures in the ROC have been obtained.

The simple answer is, the applicant is not required to disclose this information. The applicant's obligation in presenting its evidence in the ROC is fully described in *Dotcom v USA* paras [153] and [190]. There is not a breach of the duty of candour and good faith.

- (vii) The first respondent refers to para 148(b) of the 4<sup>th</sup> SROC where the ROC alleges:

“On or about August 16, 2010, via Skype, DOTCOM told ORTMANN in German, “at some point a judge will be convinced about how evil we are and then we’re in trouble. We have to make ourselves invulnerable”. To prevent this possibility, DOTCOM suggested “a new hosting model” that would make Megaupload “independent from,” its server hosting facilities, “Carpathia or Leaseweb”. DOTCOM said that Megaupload “should set up a fleet of our own servers with multiple hosters (15 or more in several countries) and make us untouchable”. DOTCOM was particularly concerned about the domain name, stating, “The domain is the only danger, but for that there is the megakey”.

The first respondent has had another translation done of this conversation from German to English, and says the correct translation is:

“Because at some stage a Judge will be talked into how bad we allegedly are and then it will be a mess. We must make ourselves invulnerable, the only danger then will be the domain but to avert this we’ve got the Megakey”.

The first respondent submits that the translation in the ROC is incorrect and material has been left out to deliberately create a different and more sinister impression.

This Court is not in a position to decide which translation is correct or more correct than the other. Nor does it need to. A difference in translation is a trial issue. If the translation obtained by the first respondent was assumed to be the correct translation, there remains more than sufficient evidence to establish a prima facie case. The decision of this Court does not rest upon the translation of this skype conversation. Their disputed translation does not provide evidence of a breach of the applicant’s duty of candour and good faith.

- (viii) It is submitted by the first respondent that the reliability of the ROC is seriously compromised as it includes a collection of skype and email communications without identifying the means by which they were obtained. It is submitted that there is no way of knowing whether they were obtained lawfully or unlawfully. It is further submitted that evidence was obtained from cloned hard drives found to have been removed from New Zealand unlawfully in *Attorney-General v Dotcom*.<sup>181</sup> Further, it is submitted that the applicant has omitted key passages from the communications in order to convey an entirely different meaning. The first respondent concludes that the absence of evidence leads to the conclusion that the applicant has been less than candid.

The issues raised in *Attorney-General v Dotcom* have already been dealt with by the Court of Appeal. The applicant is not required to identify how its evidence was obtained. Submissions that the applicant has selectively picked its evidence are just submissions and do not amount

---

<sup>181</sup> *Attorney-General v Dotcom* (Search Warrants) [2014] NZCA 19 at [114].



to evidence that there is a basis for finding a breach of the duty of candour and good faith.

- (ix) It is the first respondent's submission that the applicant's case is built almost entirely on inferences. This Court has reviewed the evidence adduced from the ROC and is satisfied that when inferences are required in order to establish a prima facie case then they are based upon evidence from which it is reasonable to draw those inferences. There is no breach of the duty of candour and good faith here.
- (x) The second and third respondents submit that this Court has been misled as to the operation of the internet in general and cloud storage facilities in particular. They point to the evidence of Professor Sallis and say his evidence differs in some areas from that given by FBI representatives in the ROC.

The evidence of Professor Sallis was particularly useful to the Court by putting the operations of the internet and cloud storage into an overall understandable context. However his evidence does not undermine the evidence of the ROC to an extent that the ROC evidence is unreliable. His is an alternative view that might be applicable at trial. It is not the role of this Court to decide which expert is more correct. Accordingly there is no breach of the duty of candour and good faith. That is a trial issue.

- (xi) The second and third respondents submit that the failure of the applicant to disclose that the movie "Taken" was:
  - (a) released to cinemas in 30 countries by 25 October 2008; and
  - (b) likely to have been distributed on DVD in at least 8 countries prior to 25 October 2008

and further, has given no evidence as to whether:

- (c) Mr van der Kolk or the alleged recipient of the email were in the USA on 25 October 2008; or
- (d) the file was uploaded by users in the USA prior to the release of “Taken” in the USA

is a misrepresentation amounting to a breach of the duty of candour and good faith.

The evidence that Mr van der Kolk uploaded the movie “Taken” on 25 October 2008, it was covered by copyright in the USA at that time and was available for downloading from Mega from that date does not appear to be disputed. No evidence is given that the applicant knew of the distribution of “Taken” in some countries outside of the USA, although that inference might be drawn. What is relevant is the alleged conduct of Mr van der Kolk. Did he make the movie “Taken” available to users in countries where it had not been released in breach of the copyright owners’ proprietary rights? That is a trial issue.

The second and third respondents’ submissions do not amount to a breach of the applicant’s duty of candour and good faith.

- (xii) The second and third respondents submit that the provisional arrest warrants issued by McNaughton DCJ nearly four years ago were made on an ex parte application. That application was supported by affidavits representing that information concerning the likely movements of the suspects had been obtained as a result of interceptions conducted by the FBI. They submit McNaughton DCJ was not informed that the GCSB had been assisting the applicant and the police by conducting unlawful surveillance on New Zealand residents to obtain information on their likely movements. It is submitted that in obtaining the provisional arrest warrants the applicant has misled this Court and therefore acted in breach of its duty of candour.

- (xiii) The provisional arrest warrants were issued almost four years ago. They do not impact upon whether this eligibility hearing is fair nor the respondents prejudiced in their defence. It is not a breach of the duty of candour before this eligibility Court.

The applicant's submissions on a question of law such as transposition is a legal issue before this eligibility Court that the applicant has a different view of the law from the second and third respondents' counsel is not a breach of the duty of candour.

- (xiv) There is no basis for the contention that an extradition cannot result from a test case. By definition, every type of case when heard for the first time could be classified as a test case. The conduct alleged by the applicant against the respondents either results in eligibility for extradition or it does not. In any event there are similar cases including *Griffiths v USA*,<sup>182</sup> *The Twentieth Century Fox Film Corporation v Newzbin*<sup>183</sup> and others that cover similar issues. There is no breach of the duty of candour and good faith based upon novelty.

### **Duty of Candour and Good Faith**

[689] Throughout their submissions the respondents have raised many instances of what they claim to be a breach of the duty of candour and good faith by the applicant. All have been considered but not all referred to in this decision. They have been raised mainly for matters upon which the applicant and respondents have different points of view, a relitigation of matters already decided upon by New Zealand courts, or are accusations about matters of no relevance to this eligibility hearing. This Court is satisfied that none of the submissions made individually or submissions made if considered in their entirety come close to establishing a breach of the duty of candour and good faith.

[690] Differences of opinion, disputing minor matters of evidence and making accusations without an evidential background do not provide any basis for

<sup>182</sup> *Griffiths v USA* [2004] FCA 879.

<sup>183</sup> *The Twentieth Century Fox Film Corporation v Newzbin* [2010] EWHC 608 (Ch).

establishing a breach of the duty. The applicant has produced a very substantial ROC in support of this application. It would be surprising if there were not some parts of that ROC that was not contested. The respondents' submissions fall well short of undermining the applicant's case or showing it to be unreliable. The large body of evidence in the ROC and its supplements that support the establishment of a prima facie case remain intact.

### **Restrictions on Surrender**

[691] It has been submitted for the first respondent, Mr Dotcom, that if this Court was to find a prima facie case against him rendering him eligible for surrender, then the mandatory restrictions on surrender in s 7 and the discretionary restrictions in s 8 of the Act should be applied by this Court.

[692] Section 24 says at subs (3) and (4):

- (3) The person is not eligible for surrender if the person satisfies the court-
  - (a) that a mandatory restriction on the surrender of the person applies under section 7; or
  - (b) except in relation to a matter referred to in section 30(2)(ab), that the person's surrender would not be in accordance with the provisions of the treaty (if any) between New Zealand and the extradition country.
- (4) The court may determine that the person is not eligible for surrender if the person satisfies the court that a discretionary restriction on the surrender of the person applies under section 8.

[693] Section 7 of the Act says:

#### **7 Mandatory restrictions on surrender**

A mandatory restriction on surrender exists if—

- (a) the offence for which the surrender is sought is an offence of a political character; or
- (b) the surrender of the person, although purportedly in respect of an extradition offence, is actually sought for the purpose of prosecuting or punishing the person on account of his or her race, ethnic origin, religion, nationality, sex, or other status, or political opinions, or for an offence of a political character; or
- (c) on surrender, the person may be prejudiced at his or her trial or punished, detained, or restricted in his or her personal liberty by

reason of his or her race, ethnic origin, religion, nationality, sex, or other status, or political opinions; or ...

[694] Section 8 of the Act says:

**8 Discretionary restrictions on surrender**

- (1) A discretionary restriction on surrender exists if, because of—
- (a) the trivial nature of the case; or
  - (b) if the person is accused of an offence, the fact that the accusation against the person was not made in good faith in the interests of justice; or
  - (c) the amount of time that has passed since the offence is alleged to have been committed or was committed,—
- and having regard to all the circumstances of the case, it would be unjust or oppressive to surrender the person.
- (2) A discretionary restriction on surrender exists if the person has been accused of an offence within the jurisdiction of New Zealand (other than an offence for which his or her surrender is sought), and the proceedings against the person have not been disposed of.

[695] Mr Dotcom through his counsel's submissions and his affidavit filed in support of his evidence during the hearing of the stay application during this hearing, alleges that the United States movie studios provide very large sums of money to the Democrat and Republican political parties, and to the Democrat Party in particular. The present President of the United States of America is a Democrat. He alleges that highly placed US movie studio executives have often met with highly placed US politicians, including the Vice President of the United States of America, Mr Joe Biden. He says that his views on the use of the internet and its future use is very different from the views of the US movie studios and he is being attacked by them because of his views. In essence he is alleging the US movie studios have used credit they have built up with the Democrat Party administration in the USA to have him extradited from New Zealand to face prosecution in the USA. He submits that the prosecution of him has a political motive and this Court should use its discretion to stop his surrender for extradition.

[696] The primary application which is the subject of this hearing has already been found to have a legal basis as a prima facie case has been established by the applicant. The charges are not trivial in nature pursuant to s 8(1)(a) as they allege serious misconduct involving approximately US\$175 million claimed to be lost by

the copyright owners. As a prima facie case exists, it is proper that the copyright owners should be heard at trial.

[697] That Mr Dotcom has a different point of view about the use of the internet from others including the US movie studios does not have the hallmarks of what is ordinarily regarded as political persecution for political beliefs. It is a difference of opinion about a business matter, the use of the internet and the application of copyright law. There is a prima facie case providing a legal basis for his extradition for these issues to be heard at trial. There is therefore no basis for finding the first respondent not eligible for surrender based upon either sections 7 or 8 of the Act.

### **Conclusion**

[698] This eligibility Court has received an extraordinarily large volume of material to consider, and the hearing took over 9 weeks before completion. The parties were informed by this Court that all matters relevant to this eligibility hearing would be heard at the hearing and decisions would issue accordingly. At the end of the hearing, all parties confirmed to this Court that none of them had any further issues they wished to raise.

[699] Given the very large volume of material presented during the hearing it is not possible to issue decisions that would be less than encyclopaedic in length in order to cover every minor point alluded to in the hearing. There is no need to do this. Much of the material presented to this Court has not been relevant to an eligibility hearing and a number of the submissions were unsupported by appropriately sworn evidence. They do not come near to undermining the applicant's case or point to a breach of the duty of candour and good faith. If some aspects of the parties submissions or evidence has not been referred to in this judgment that is because it was not relevant to the decision given.

[700] The overwhelming preponderance of evidence produced by the applicant in the ROC and the SROC establishes a prima facie case to answer for all respondents on each of the counts.

[701] Pursuant to s 24(1) this Court finds that the respondents are all eligible for surrender on all thirteen counts in the superseding indictment.

N R Dawson  
District Court Judge