IN THE DISTRICT COURT
AT NORTH SHORE

KIM DOTCOM
Applicant

v

UNITED STATES OF AMERICA
Respondent

Hearing: 23 January 2012

Appearances: Mr Davison QC and Ms Woods for the Applicant
Ms Toohey and Mr Sinclair for the Respondent

Judgment: 25 January 2012

RESERVED JUDGMENT OF JUDGE D J McNAUGHTON
[Opposed Bail Application]

---

[1] The United States of America is seeking to extradite Mr Kim Dotcom from New Zealand. An indictment has been filed in the District Court for the Eastern District of Virginia charging Mr Dotcom and others with:

- Conspiracy to commit racketeering.
- Conspiracy to commit copyright infringement.
- Conspiracy to commit money laundering.
- Criminal copyright infringement by distributing copyrighted work being prepared for commercial distribution on a computer network and aiding and abetting of copyright infringement.

- Criminal copyright infringement by electronic means and aiding and abetting of copyright infringement.

[2] I record that pursuant to s 20 of the Extradition Act 1999 I issued a provisional arrest warrant for Mr Dotcom and others on 18 January 2012 and then the following day, warrants to search a number of addresses including Mr Dotcom's residential address at Coatsville.

[3] I was prepared to disqualify myself from hearing the bail application if counsel were concerned regarding any possible conflict of interest or actual or apparent bias but all counsel were content for me to deal with the bail application.

[4] Presentation of the indictment follows a lengthy FBI investigation which commenced in March 2010. The FBI alleges that the applicant and others are involved in a worldwide criminal organisation known collectively as the Mega Conspiracy. There are seven persons targeted by the investigation and charged in the indictment. Mr Dotcom and Bram van der Kolk both reside in New Zealand. The remaining five defendants are resident in Europe and Hong Kong. Mr Dotcom is a 68% shareholder in a company called Mega Upload Limited the registered owner of Mega Upload.com allegedly the main website used to facilitate the operation of the Mega Conspiracy.

[5] The prosecution allege the business is run from servers in the Netherlands, Canada and the United States. Charges are laid in the United States on the basis that a large portion of the servers are located there but the prosecution assert the business could be run from any location and the seven alleged conspirators need not be proximate to the servers.

[6] Mega Upload.com claims to account for an estimated 4% of all internet traffic worldwide and to attract 50 million visits a day. The business is also highly profitable. Restraining orders have been issued in the United States for assets including some assets held in New Zealand valued at US$175 million, allegedly criminal proceeds acquired as a result of criminal offences.

[7] Section 43(1)(b) of the Extradition Act 1999 provides that the provisions of part 1 of the Bail Act 2000 are to apply in respect of proceedings brought under the Act and therefore it is for the Crown to show that there is just cause for continued detention taking into account the mandatory and discretionary factors set out in s 8 of the Bail Act. Bail is opposed by the Crown primarily on the basis that Mr Dotcom is an extreme flight risk and also that there is a risk of reoffending on bail.

Flight Risk

[8] It is submitted that when the police executed the arrest and search warrants on the morning of 20 January 2012 that Mr Dotcom attempted to evade arrest by activating a sophisticated security lock on his bedroom door and then retreating to a second "panic room" hidden within his bedroom again secured by a security locked door and when the police gained entry to this room Mr Dotcom was present and there was a loaded shotgun in a nearby safe.

[9] It is noted that Mr Dotcom does not hold a firearm licence and that his bodyguard Mr Wayne Tempero has been charged in relation to an identical firearm found in a gun safe in a room occupied by him in an adjacent building. Mr Tempero holds a firearm licence, but not to that particular category of firearms.

[10] The firearm is described as a pistol grip shotgun with a removable stock which had been detached and placed in the safe alongside. There were four rounds loaded into the shotgun with another five twelve gauge shotgun rounds attached to the firearm. There was a shell in the breach which was a rubber round and a different colour from the remaining rounds which were all red and contained buckshot.

[11] It is accepted that Mr Dotcom had access to a number of bank accounts including 23 separate bank accounts in Hong Kong, 15 with the DBS Bank and 8 with Citibank exceeding NZ$26 million.

[12] The FBI allege that Mr Dotcom has registered bank accounts in the Philippines and the United Kingdom, a credit card in Germany and multiple

additional limited liability companies registered under various aliases in different countries. It is asserted that his income for the calendar year 2010 was approximately US$42 million. In addition the applicant has $10 million in government bonds in various New Zealand accounts which are also restrained property. The FBI alleges that the various accounts which are known and restrained do not represent all of the funds available to Mr Dotcom and that there is a significant possibility that other financial resources are available to him.

[13] In 1998 the applicant was convicted in relation to computer hacking committed in 1994 and was sentenced to two years imprisonment suspended for two years. In 2003 in Germany he was convicted of insider trading and breach of trust committed in 2001 and sentenced to one year eight months imprisonment suspended for two years. Finally there is a conviction in 2011 in Hong Kong for failing to publically disclose the number of shares acquired in 2009. Mr Dotcom was fined a total of HK$8,000 and ordered to pay investigation costs of HK$17,421 to the Securities and Futures Commission.

[14] The prosecution placed considerable emphasis on events leading up to the 2003 conviction in Germany alleging that Mr Dotcom fled Germany in a response to an investigation there in 2001 and 2002 to Thailand and was later arrested and eventually deported to Germany. The prosecution submitted that this demonstrated that the applicant is a considerable flight risk.

[15] Mr Dotcom holds a number of passports. One is a German passport in the name of Kim Schmitz which is his original name. That passport was issued in 2002 and expires in May 2012. He holds another passport issued in Finland in the name of Kim Tim Jim Vestor in 2005 which expires in July 2015 and finally another passport issued in Finland in the name of Kim Dotcom in 2010 which expires on 12 February 2015.

[16] One of the applicant's New Zealand accounts ASB account no. 12-3170-0066521-00 is in the name of Kim Tim Jim Vestor. The FBI alleges that the applicant is actively maintaining alternative identities complete with funds and travel documentation.

[17] An affidavit was filed by Malcom Spence a detective with the Asian Crime Unit explaining how a Chinese national sought for extradition to the United States and subject to daily reporting, and surrender of travel documents had disappeared prior to the hearing of the request for surrender for extradition.

[18] I record that the respondent had also filed an affidavit from a senior customs official explaining the availability of false passports and travel documentation at a price. The affidavit described porous nature of New Zealand's boarders should the applicant chose to leave the country by boat or an airport or airstrip outside the main centres and the mechanics of organising travel to Australia or other South Pacific countries by small aeroplane, yacht or commercial vessel.

[19] The respondent was concerned that this material not fall into the public domain and I heard submissions in relation to the affidavit in closed Court. The prosecution were concerned that this material might be accessed from the Court file and so the original affidavit was returned to the prosecutor.

[20] It is submitted that Mr Dotcom maintains residences in both New Zealand and Hong Kong and that his address at Suite 3608, Grand Hyatt Hotel, Hong Kong is a permanent address.

[21] It was submitted that Mr Dotcom has in the past used chartered private jets, helicopters and yachts including leasing a helicopter for a month in 2010 together with a pilot on a retainer.

Risk of Offending on Bail

[22] It is submitted that the applicant's business is compact involving the seven alleged conspirators and a total worldwide staff of 30. A computer server is required to maintain the various websites and the business is able to be run at a distance given that the various alleged conspirators reside in Hong Kong, New Zealand, Germany, Estonia and Slovakia whilst the websites themselves are operated through servers in the United States of America, Netherlands and Canada.

[23] Four of the alleged conspirators were arrested and detained in New Zealand. A fifth defendant named Nomm in the indictment was arrested in the Netherlands on a provisional arrest warrant. A sixth defendant named Echternach was in the Philippines at the time the warrant to arrest was executed but has since travelled to Germany which has no extradition treaty with the United States and Ms Toohey advised that Germany will not extradite German nationals to the United States.

[24] It was submitted that if Mr Dotcom were granted bail he would assist the remaining two defendants still at large who may be trying to reinstate the business in some modified form from overseas jurisdictions. Various domain names have been registered in other countries outside the United States from which that business could be operated. The seventh defendant, a Mr Bencko who is still at large, attempted to contact Mr van der Kolk by telephone as the police were executing the warrant at Mr van der Kolk's address on the morning of 20 January 2012.

[25] There is a huge demand for the business given the volume of internet traffic and the number of visits to the site per day, estimated at 50 million. It is submitted that the vast profits generated are a further incentive to restart the business from another location. In response to the taking down of websites in the United States various hacker groups have attacked government sites in response and it is submitted this also is an indicator of strong demand.

Section 8(2) Discretionary Factors

[26] It is submitted that this is the largest prosecution to date for infringement of copyright in the United States. The offending is described as unprecedented and most serious. The conspiracy to commit racketeering and money laundering charges carry maximum penalties of 20 years imprisonment and Ms Toohey is instructed that prosecutors in the United States will press for the maximum penalty if the defendants are convicted.

[27] It is acknowledged that no assessment of the strength of the evidence can be made at this point. Supporting evidence will be filed along with the request for surrender.

[28] Under the heading of character and past conduct or behaviour I was asked to take into account that in 2006 Mr Dotcom participated in a gumball rally event in which he was driving at speeds of 250 kph and refused to stop at a police check point when motioned by an officer to pull over to the side of the road. For the purposes of this bail application I place no weight on that whatsoever. Further, any suggestion that Mr Dotcom was actively avoiding or resisting arrest by sitting on the floor cross legged when the police entered the inner panic room, and failed to immediately stand and show himself, I dismiss also.

[29] In relation to delay the request for surrender for extradition must be made within 45 days of the arrest. Once the request is received extradition proceedings will be filed and a hearing date set. Ms Toohey indicated that that hearing might take a day given the pro forma nature of the evidence in a summary form. At this point I am unable to determine precisely how long the hearing would take but even if it were a full day this Court could not accommodate such a hearing for some months.

Defence Submissions

[30] Mr Dotcom in his affidavit emphatically denies any criminal misconduct. He denies the existence of the so-called Mega Conspiracy and denies that there was any criminal enterprise relating to reproduction and distribution of infringing copies of copyrighted works via the internet. He deposes that Mega Upload is essentially a file storage facility available to internet users to upload their own digital files and users are provided with a link which enables other users access to those digital files. The terms and conditions of access to the storage facility stipulate the prohibition on any uploading of any digital material or files in which the user is not the legal and authorised owner of the copyright. It is noted that privacy laws prevent searching of the digital files by Mega Upload but it is recognised that some users have and will upload films, videos and other copyrighted material in order to share those files with other internet users.

[31] Mega Upload has negotiated with major rights holders including The Recording Industry Association of America, The Motion Picture Association of America, Disney, Warner Bros and Universal Pictures and others a facility enabling

these organisations to take down or remove files breaching their copyright directly and without prior reference to Mega Upload. In accordance with the US Digital Millenium Copyright Act Mega Upload has met requirements to remove any offending items uploaded to the site within 24 hours notice received from the relevant copyright holder. This does not apply to internet users outside the jurisdiction of the United States.

[32] Mr Dotcom states that there have been some 15 million take downs either conducted by Mega Upload pursuant to take down notices or files taken down directly by the copyright holders.

[33] It is noted that there are some 12 billion files stored and that the proportion of digital material infringing copyright is relatively small. He states that the vast majority of Mega Upload users use the storage facility for entirely legitimate storage of personal and business related files.

[34] Whilst the alleged gross revenue of $175 million over the past five years is not disputed business expenses account for 50% of the gross revenue.

[35] Mega Upload has employed sophisticated and expensive systems that prevent search engines such as Google "crawling" over its database and indexing its file both to protect the privacy of its users and to prevent other internet users accessing material that breaches copyright.

[36] In answer to the US Government submission that a user rewards programme was introduced to increase the illegal downloading of files breaching copyright. Mr Dotcom states that the rewards programme had been in place at an early stage and only paying members were entitled to receive rewards and paying members were required to provide identification details. He states that the provision of identification details was a disincentive for users to share files in breach of copyright and in any event the rewards programme was discontinued in 2011 and notwithstanding that withdrawal usage of the site has continued to increase.

[37] Mr Davison submitted that the nature of the offending had been amplified beyond reality and that there was a complete misapprehension on the part of the US Government regarding the true nature of the applicant's business and that there is no concession regarding the cogency of the government's case.

Flight Risk

[38] Contrary to the US Government's submission that the applicant is an extreme flight risk Mr Davison submitted he presented no flight risk whatsoever. He submitted that the operations of Mega Upload had been effectively terminated by seizure of the requisite servers in the United States and data storage equipment and restraint of assets and business accounts held by Mega Upload and the applicant personally.

[39] Mr Davison submitted there was no ability, let alone financial incentive, to start the business again and that the applicant has no interest in restarting the business until these charges are resolved. He submitted that millions of dollars had been spent on legal advice to ensure that Mega Upload was operating within the law.

[40] The applicant in his affidavit disputed any suggestion that he was attempting to evade the police or avoid arrest. He states that there were concerns for the personal safety of himself and his family and that "security protocols" were in place. In closed Court Mr Davison explained the position regarding possession of the firearm submitting that the applicant's wife is from the Philippines where kidnapping of wealthy individuals or the children of wealthy individuals is a common place occurrence and that the applicant's retention of a bodyguard and acquisition of two firearms were a precautionary measure to meet that threat.

[41] The security system in place in the applicant's bedroom and the inner panic room were installed by the previous owner of the property. In his affidavit Mr Dotcom describes the inner panic room as large, about 20 metres long, and that the gun safe containing the shot gun was some distance away from where he was seated. The stock was disconnected and it was his instruction to his security advisor

that the shotgun be loaded with a rubber cartridge. The applicant acknowledges that he was not a licensed firearms holder but was intending to apply for a license.

[42] It was emphasised in the affidavit and submissions that he made no move to use the firearm and he did not resist arrest although some physical force was used to restrain him.

[43] Mr Davison described the execution of the arrest warrants by the police as unnecessarily aggressive and irresponsible and he submitted there was no basis to anticipate any physical resistance or lack of co-operation.

[44] Taking into account the nature of the charges and the applicant's limited criminal history it is difficult to disagree with that submission but the finding of this loaded unlicensed firearm in close proximity to a certain extent justifies the scale and strength of the police operation, after the event.

[45] Preliminary inspection by the police armourer suggests that the firearm had been modified in some way to reduce the length of the barrel to 300 mm and it was submitted that the firearm could not have been legally purchased in New Zealand. At a total length of 760 mm it meets the definition of a pistol.

[46] Mr Davison during the course of argument offered to call Wayne Tempero the security advisor as a witness or alternatively file an affidavit to the effect that he purchased the firearm from a firearms dealer or broker and that Mr Tempero was in the process of applying for the appropriate pistol license. In the limited time available I have been unable to resolve that issue, but in any event whether the firearm was modified or not, it was loaded, unlicensed and available and that is a significant concern.

[47] As to the use of private transport including chartered jets that is acknowledged but it is noted that charter companies and pilots are required to ensure that customs formalities are met and in any event restraint of the applicant's bank accounts in effect means that he no longer has the wherewithal to obtain private air travel.

[48] The applicant vigorously contested the assertion that he had fled Germany to avoid prosecution. His affidavit explains that he became involved in a proposal to invest €1.4 million in shares in an internet based company though a venture capital company. He only became aware that charges had been laid against him in Germany whilst on holiday in Thailand on the basis of insider trading. At that time he was interviewed by a television journalist and suggested in the course of the interview that "if young business entrepreneurs like me in Germany were being treated in this fashion I would consider living elsewhere".

[49] Mr Dotcom states that this was a comment on the business environment in Germany and the manner in which he had been treated rather than any indication that he was unwilling to return to Germany to face the charges but following the interview a warrant for his arrest was obtained by the German authorities. The German Embassy in Thailand then required the applicant to surrender his German passport which he did and at that point he was immediately informed by the Thai authorities that without travel papers he was required to leave the country. The applicant states he agreed to return to Germany accompanied by two German police detectives. He disputes that he was deported and it is emphasised that no charges had been laid at the time he left Germany and he did not leave in order to avoid prosecution. He was away for a fortnight's holiday intending to return in any event.

[50] In relation to previous convictions Mr Dotcom's affidavit notes that the German convictions are subject to the equivalent of a "clean slate" provision that the earlier hacking charges occurred when he was still a teenager. It is acknowledged that the applicant was convicted of insider trading and also misuse of business funds which arose from payment of legal fees from company funds without regard to the interest of another 5% investor. The conviction in Hong Kong related to purchase of shares exceeding a 5% threshold and requirement to notify the applicant's interest. The actual figure was 5.1% and a fine imposed on the basis of what the applicant describes as a minor regulatory breach which was unintentional and effectively an oversight.

[51] The use of aliases is explained on the basis that Kim Schmitz is the applicant's birth name which he changed following the hacking convictions to Kim

Tim Jim Vestor as a Finnish national and he was issued with a Finnish passport. He changed his name again from Kim Tim Jim Vestor to Kim Dotcom currently travelling on the Kim Dotcom passport. The applicant states that he believed the earlier Finnish passport had been cancelled and that in recent times he has consistently used the name Kim Dotcom.

[52] Mr Dotcom was granted permanent residency in December 2009. He and his family have lived here more or less continuously since September 2011. There are three children under five and the applicant's wife is also the legal guardian of her younger brothers aged 14 and 11. The applicant accepts that he maintains an apartment in Hong Kong although the lease is shortly to expire. He leases the large property at Coatsville and has an option to purchase. He employs a total of about 50 staff, it is his intention to reside here permanently and to raise his family here and his wife's brothers are enrolled at a local school.

[53] The applicant accepts that he had planned to travel to Hong Kong for a couple of months because his wife's obstetrician is based there but it was always intended that after her twins were born (and she is in the advanced stages of pregnancy) that she and the applicant would return to New Zealand.

[54] Mr Dotcom in his affidavit emphasises that there is no ability to reinstate Mega Upload.com and that during the course of the police operation executing the warrant to arrest he made no attempt to access any computers or the company servers and in any event the server at his residence is used for internal systems at the house and is not related to Mega Upload.

[55] In summary the applicant's position is that he has a good defence to any criminal charges and also any civil allegations alleging breach of copyright. He will contest the extradition but has no intention of leaving the country in the meantime. Bail is sought in order fully prepare his defence. The applicant suffers from diabetes and hypertension and is prescribed medication for both conditions. He is also receiving treatment for a slipped disc. It is submitted that a remand in custody would cause difficulties without access to proper treatment and that a delay of some months is likely pending the extradition hearing.

US Government's Reply to Defence Submissions

[56] As the argument developed the allegation of flight from Germany to Thailand assumed some importance. The only additional information offered by the US Government was sourced from a Major General in the Thai Police who indicated that the applicant was arrested and taken into custody and deported from Thailand in 2002. Mr Davison was provided with a copy of the source document, apparently a request from the US Government to the German authorities seeking details of the alleged deportation. There is no available file as such and in the end this rather terse description from the Deputy Commissioner of the Investigation Bureau with the Royal Thai Police is broad enough to fit either scenario. I cannot be certain that the applicant did in fact flee the jurisdiction and neither am I satisfied that he was deported in a legal sense.

[57] In relation to the risk of reoffending Ms Toohey referred to the indictment at page 44, paragraph UUU which refers to an email sent by Mr Dotcom to two of the named co-defendants Ortmann and Echternach on 8 July 2010. The email contained a link to a new article entitled "Pirate Bay and Mega Upload Escaped Domain Seizure by US". The article discussed a crackdown by the US Government against internet piracy and counterfeiting which the applicant described in the email as "a serious threat to our business". He suggests that his co-defendant investigate the issue and look at how the business could be protected and asked whether "we move our domain to another country Canada or even Hong Kong".

[58] Mr Davison submitted that there were real concerns on the part of Mr Dotcom and his associates, that the site could be taken down by the authorities. Mr Davison submitted those concerns did not arise from any illegal activity but rather an apprehension that the US Government might act precipitously without any opportunity for the applicant to explain and defend his position and that those fears have now been realised.

[59] Ms Toohey in her submissions in reply rejected any suggestion that the business of Mega Upload is simply file sharing referring to the rewards system described in the indictment at page 29, paragraph E. An early version of the programme was announced in September 2005 paying money and cash to uploaders the minimum qualification was 50,000 downloads within three months and permission to list those files and descriptions on Mega Upload's top 100 pages. The rewards included $1 per 1,000 downloads and bonuses of between $50 and $5,000 to the top 100 Mega Uploaders with the most downloads during the three month period.

[60] Mr Davison submitted that the reward system was nothing more than good business practice to reward creative effort and that there was no intention to encourage breach of copyright.

[61] Ms Toohey submitted that files uploaded to Mega Upload.com were each assigned a unique identifier called a "MD5#" described in the indictment at page 10, paragraph 22. Ms Toohey submitted that that unique identifier had been used to identify child pornography and terrorist material. She submitted that whilst copyright holders were able to delete URL links to a particular file (the so called take down) nonetheless the files themselves still existed and in relation to 39 motion pictures stored in files uploaded to Mega Upload.com infringing the owner's copyright, 36 of the 39 motion pictures were still held in digital files two years after receipt of the take down notices.

[62] Mr Davison submitted that whilst use of the MD5# identifier was effective in removing offensive material such as child pornography in a specific search exercise, to apply the same process to all digital files was equivalent to using an antibiotic for every medical complaint and that ultimately that process would be ineffective and users would quickly find ways to circumvent it. He submitted that location and reporting of child pornography demonstrated corporate responsibility on the part of the business.

[63] Ms Toohey referred to an email sent by the applicant to co-defendants van der Kolk, Ortmann and Bencko on 23 April 2009 complaining about the deletion of URL links in batches of thousands from insignificant sources.

> I would say that those infringement 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.

[64] The following day the applicant sent a further email referring to a steep drop in revenue caused by mass link deletions and insisted that there should be careful checking of sources and not to delete thousands of links at once from a single source unless it came from a major organisation in the United States. Ms Toohey submitted the emails demonstrate a selective approach to compliance with copyright infringement.

[65] Mr Davison submitted that there were unauthorised take down requests lodged by competitors seeking to obtain a commercial advantage and that the applicant was simply concerned at verification of take downs by bona fide major operations in the United States as opposed to other commercial interests, for example from Mexico.

[66] Ms Toohey referred to page 42, paragraph LLL of the indictment which refers to a complaint by Warner Bros Entertainment Inc that Warners were unable to remove links and requesting an increase in the removal limit. The applicant received an email from Mr Ortmann dated 10 September 2009 advising that Warners were removing 2,500 files a day which he described as legitimate take downs of content they own appearing in public forums and that the requests should be complied with. The applicant agreed to increase the limit to 5,000 per day "but not unlimited".

[67] Returning to the issue of flight risk Ms Toohey then referred me to some additional material prepared by the FBI opposing bail. At page 4 of the document is an extract from a Skype chat log between van der Kolk and Ortmann dated 21 August 2007 in which van der Kolk states:

> 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.

[68] Ortmann responds:

> The good thing is he is operationally dependant on us . . . he cannot sneak away with the money.

[69] Van der Kolk then asks:

> But what if the shit really hits the fan . . . would he grab the last little bit of money and take off . . . he's good at that.

[70] Ortmann then states:

> True but with his spending now days he will attempt to get the shit off the fan and that's what he needs us for.

[71] Ms Toohey submitted that the scenario discussed between the applicant's close associates in 2007 was now a reality and that the mistrust expressed by the applicant's close associates was well founded and a reliable indicator of his likely response if released on bail.

[72] Mr Davison emphasised the date of the discussion some four and a half years ago. He urged that these conversations not be taken out of context or elevated into a firm conclusion that the applicant has a propensity to avoid his lawful obligation.

[73] Finally it was submitted that in addition to the passports found in the applicant's possession he was also holding 16 credit cards in one wallet and nine in another. Mr Davison submitted that most of those cards were out of date and that the applicant was a "collector" of credit cards and that there was nothing significant in the location of either the credit cards or the passports.

Findings

[74] The starting point is s 8 of the Bail Act. It is for the prosecution to establish that there is just cause for continued detention. Flight risk and the risk of reoffending on bail are mandatory considerations.

[75] In relation to the offences charged in the indictment whilst the maximum penalties for the money laundering and racketeering offences are 20 years imprisonment the copyright charges are relatively less serious carrying maximum penalties of five years imprisonment.

[76] I am mindful of the scale of the offending described in the indictment and that this is the biggest case of its kind ever prosecuted in the United States. I cannot be sure as to the ultimate penalty if the applicant were convicted and Counsel were not able to assist me with any relevant sentencing decisions relating to breach of copyright from the United States but taking into account the nature and duration of the alleged offending and the profits generated from it, it is safe to assume that substantial terms of imprisonment would be imposed although whether those sentences would be anywhere close to the maximum available penalties of 20 years I simply cannot say at this point.

[77] As to the strength of the prosecution case I am in no position to assess that as the evidence has not yet been filed. I am asked to determine that issue on the basis of the indictment, the summary of facts and counsel submissions regarding the respective merits. It is simply impossible for me to determine at this very early stage whether the US Government has a strong case or whether the applicant has a good defence to any or all of the offenses charged. All I can say is that there appears to be an arguable defence at least in respect of the breach of copyright charges and no doubt very considerable resources will be brought to bear both for the prosecution and the defence should the matter proceed to trial.

[78] As to the applicant's ability to flee the jurisdiction I am sure that he has the financial resources to obtain forged identity or travel documents and to arrange transport out of the country by covert means should he chose to do so. I very much doubt the form of transport would be chartered jet or helicopter and previous use by the applicant of either chartered jets or helicopters is essentially irrelevant. Mr Davison acknowledged in his submissions that the applicant holds another account in New Zealand unknown to the FBI with a balance of NZ$300,000. The applicant disclosed the account and the funds it contained as a sign of good faith in advancing his bail application. I cannot exclude the possibility that there are other bank accounts and other sources of cash available to him at short notice.

[79] The real question though on the bail application is whether there is any incentive to flee the jurisdiction. If the applicant were able to leave the country undetected and travel to Germany he would be safe from extradition to the United

States. The US Government submits the risk of flight is extreme. The applicant submits the risk is non-existent. Given the nature of the business of Mega Upload.com and the profits it generated and the discussions some years earlier regarding shifting the domain to Canada or Hong Kong I would be surprised if the applicant and his close associates had not already discussed the possibility of legal action either in the Civil Courts by copyright holders or criminal prosecution. I would expect that there are already contingency plans in place should Mega Upload.com be closed down in the United States involving back up storage of data and transfer of data to another website outside the jurisdiction and that remains a real possibility whether or not the applicant is released on bail because there are still some 30 staff employed worldwide and two of the seven named defendants are still at large.

[80] The alleged risk of reoffending then is a neutral factor on this bail application. Restarting the business from another site outside the jurisdiction is a factor completely outside the Courts control, and remains an open question irrespective of any decision regarding bail.

[81] The value of the restrained assets is massive and there must be strong financial incentive to defend the criminal charges and undermine any claims for confiscation based on money laundering or racketeering. The applicant and his associates have been operating in plain sight for some years. Prosecution for breach of copyright must have been an ever present possibility and if that is the applicant's view of the matter I can accept that there is absolutely no incentive to leave New Zealand pending hearing of the extradition.

[82] Mr Davison may well be correct when he submits that Mr Dotcom wishes to let the legal process take its course and has no desire to live as a fugitive.

[83] On the other hand I cannot discount the scenario advanced by the Crown that with the applicant's business effectively shut down in the United States and his bank accounts and assets frozen and facing prosecution on serious charges with the full weight of the United States Government behind it that the applicant may take whatever money is still available to him and run to safe haven in Germany.

[84] In making that assessment I place no weight on the so called deportation from Thailand in 2002. If the US Government had been able to satisfy me that is in fact what occurred then my decision in relation to bail would have been straightforward and I could accept the submission that the risk of flight is very significant.

[85] Similarly I place no weight on the proposed trip to Hong Kong for medical reasons relating to the pregnancy or the retention of an apartment there.

[86] While the US Government's argument on flight risk in general is not as strong as initially suggested nonetheless I am left in the position that there is a risk and it is a significant risk. The applicant has explained his possession of three passports in three different names and the reason for changing his names but the fact remains that he has no qualms about changing his identity and had up to the time of his arrest been operating at least one bank account under another name.

[87] The applicant's unlawful possession of the firearm is another factor which weighs in the balance. It suggests a level of criminality which to my mind could easily extend to exploiting criminal connections to obtain false travel documents and leave the country undetected.

[88] While there will be a delay of some months until the request for surrender can be heard that is not a factor of any real weight at this point, taking into account the nature of the charges and the potential penalties. I am mindful of the impact of custodial remand on the applicant's family, particularly his pregnant wife and the many staff he employs. I do not ignore either the medical issues or the difficulties in meeting counsel and mounting an effective defence. In the end flight risk remains a serious concern and must be taken into account in consideration of just cause for continued detention.

[89] The final issue is whether there are bail conditions which could meet that risk. The applicant offers electronic monitoring funded privately. He could be required to report to the police on a daily basis, subject to 24 hour curfew which the police could check at any time, not to apply for travel documents, and not to possess or operate any computer, cell phone or internet connection. Bail conditions

permitting search of his residence to ensure that neither the applicant, any family members or staff were in possession of computers, cell phones or able to access the internet could be imposed.

[90] Whilst those conditions would restrict the applicant's movements and inhibit his ability to plan any escape, with sufficient determination and financial resources flight risk remains a real and significant possibility which I cannot discount and bail is declined.

D J McNaughton
District Court Judge