

[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 through 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: