MegaUpload Case -- US Seeks Dominion Over Cyberspace

by Brett Winterford via Kismo - itNews *Sunday, Jan 22 2012, 8:19pm*
international / mass media / other press

Serious ramifications for ALL 'cloud' services

> *Have we had enough of America's 'permanent war,' 'indefinite detention,' neo-fascist policies or should we ALLOW the US to harness and control Cyberspace -- that is the principal issue behind the Assange and MegaUpload cases?*
>
> *Not content with illegally invading weaker nations, plundering and killing thousands of innocent civilians -- all in the name of PROFIT -- the clearly criminal US now seeks dominion over Cyberspace, the last truly FREE social space left to humanity.*

Do US borders now extend to 'incorporate' all Cyberspace and the entire planet, as the nefarious US executive wishes to achieve, or will the free WORLD wake and immediately INSIST that America OBSERVES its legal limitations and geographic borders? The Internet is the VITAL and critically important phenomena it is today due primarily to the fact that no-one OWNS it!

The new 'indefinite detention law' designating the entire planet a war zone -- in order to fulfil America's neo-fascist 'permanent war doctrine' -- makes it plain, the US seeks TOTAL GLOBAL DOMINATION of ALL social and geographic space, a lunatic ambition in the modern world if ever there was one!

It is no secret that information control leads to social control; therefore the question arises, WHERE IS THE RESISTANCE? WHERE ARE YOU CHINA/ASIA and RUSSIA; notwithstanding the free people of the world instinctively oppose all forms of oppression and totalitarian rule?

Report from itNews follows:

> Last week's arrest of MegaUpload staff in New Zealand and the possibility of their extradition to the United States raises significant questions for users of cloud services the world over.
>
> I spent the weekend discussing the ramifications of the case with Shelston IP partner Mark Vincent, a globally recognised expert on cloud computing and the law, who by good fortune also happens to be a New Zealand lawyer in Auckland.
>
> We felt it best to distil concerns around the case down to four key questions:
>
> - **Does US territory now extend to cyberspace?**
>
> - **What crime would be grounds for extradition?**
>
> - **What constitutes racketeering in an intellectual property case?**
>
> - **Could this precedent extend to other cloud services?**

While the indictment suggests the US authorities have done their share of homework on global law, they can expect to encounter some difficulties with the following aspects of the case:

1. Does US territory now extend to cyberspace?

According to the US Department of Justice, the New Zealand Police arrested MegaUpload staff in Auckland that were citizens of Finland, Germany and The Netherlands using warrants "requested by the United States."

These individuals, three other individuals that are not US residents or US citizens and two companies (Megaupload.com Limited and Vestor Limited) registered in Hong Kong, were indicted under US law for allegedly "engaging in a racketeering conspiracy, conspiring to commit copyright infringement, conspiring to commit money laundering and two substantive counts of criminal copyright infringement."

Despite the support of the Organised and Financial Crime Agency of New Zealand (OFCANZ), the Crown Law Office of New Zealand and the Office of the Solicitor General for New Zealand, the nationality and business address of the accused raise interesting questions around jurisdiction, namely: does United States territory now extend to cyberspace?

According to Vincent, for the purposes of extradition, the requirement of the New Zealand extradition treaty with the United States requires that crimes be committed within United States territory. This will create interesting issues for extradition arguments.

National jurisdiction has traditionally extended to activities that take place within a country, in its waters and airspace, even in its vessels and aircraft when they move beyond these borders. But it has not traditionally encompassed activities on foreign soil. To deal with international IP infringements on the internet the United States is going to be re-defining the boundaries of state jurisdiction.

It is not clear what links each of the accused people and organisations have to United States territory. The Megaupload business had 25 petabytes of storage and 1000 servers leased in US data centres operated by Carpathia Hosting, plus a further 36 servers leased from US-based Cogent Communications. It used Paypal to process transactions.

Is the leasing of servers in the United States enough to bring these companies and individuals under the US jurisdiction? Is having your data stored anywhere in the United States (consider your iCloud account, Hotmail or Gmail etc) considered sufficient to bring you within US jurisdiction? This could prove an interesting test.

In another case from January 2012, United Kingdom student Richard O'Dwyer was cleared for extradition to the United States [pdf] by a United Kingdom court to face copyright infringement charges over his website hosted in the United Kingdom, in circumstances where he probably didn't infringe local law. His link to the United States from a jurisdictional point of view was a ".com" domain name.

2. What crime would be grounds for extradition?

The indictment, which reveals an exhaustive investigation on the part of US authorities, lists five crimes under United States law.

- Conspiracy to commit racketeering
- Conspiracy to commit copyright infringement
- Conspiracy to commit money laundering
- Plus two variations on Criminal Copyright Infringement

The list of crimes will prove important should the United States wish to extradite these individuals to face a US court.

According to fellow New Zealand lawyer Rick Shera, the arrest warrant must have required Ministerial or consular approval. Such a warrant could be granted under New Zealand's Extradition Act if "there are reasonable grounds to believe that the person is an extraditable person in relation to the extradition country and the offence for which the person is sought is an extradition offence."

The New Zealand Government has a fairly extensive lists of crimes listed in its extradition treaty with the United States, under which it would agree to extradite a resident to the United States. It should be noted that at present, none have anything to do with copyright infringement.

Neither do the words 'racketeering' or 'money laundering' appear in the list. Piracy is mentioned, but it refers to the sea-faring kind.

According to Vincent, the only crime that comes close to a match is: *" Receiving and transporting any money, valuable securities or other property knowing the same to have been unlawfully obtained."*

It may be difficult to show that the four men arrested in Auckland: Bram van der Kolk, Finn Batato, Mathias Ortmann and Kim Dotcom, were all knowingly involved in receiving and transporting money in the United States, knowing it to have been unlawfully obtained.

A read of the indictment also suggests the racketeering and money laundering charges rest entirely on whether the defendants are found guilty of the charges concerning copyright infringement, which does not represent sufficient grounds for extradition.

According to Vincent, under Article XIII of the extradition treaty there is some protection against being extradited for offences not listed in that treaty: *"A person ... shall not be detained, tried or punished ... for any offense other than an extraditable offense disclosed by the facts on which his surrender was granted."*

This makes it hard to bring copyright infringement allegations squarely within the extradition treaty. There may yet be a barrier to the extradition.

3. What constitutes racketeering and money laundering in an intellectual property case?

The US Department of Justice equated Megaupload's Rewards Program, which "provides users with financial incentives to upload popular content and drive web traffic to the site" with racketeering, noting this was achieved using user-generated linking sites.

But that business model, from a legal sense, doesn't appear dissimilar to the services of Google's YouTube, Vimeo or any number of online content services. Many services provide financial rewards to users generating popular content, most under the

assumption that the user owns the copyright in the work. The more hits a power user gets on YouTube, for example, the larger the slice of revenue they are entitled to under Google's reward program. Is that racketeering?

"Numerous parts of Google's business model reward popular content," Vincent notes. "Isn't it possible popular content might just as often be non-infringing?"

It's interesting to note that Google now shares some of that revenue with the content industry. Could Google executives be arrested for operating YouTube if the content industry turned savage on its rewards program? When Google bought YouTube in 2006 there was no solution to the problem of uploads which infringed copyright.

Like the iiNet vs AFACT case being fought in Australia, this particular issue may come down to the notion of authorisation.

The US Department of Justice claims to have evidence to prove the accused "specifically knew [of] uploaded infringing content" and promoted links to that content.

Some of the email conversations between the accused the FBI managed to access suggest they may have deliberately turned a blind eye. In one alleged exchange within the indictment, one of the accused describes them as "modern day pirates", before another corrects him.

"We're not pirates, we're just providing shipping services to pirates," the alleged exchange reads.

The 'money laundering' charges, on the other hand, appear to rest on payments allegedly made by US citizens to Megaupload from US-based vehicles such as PayPal to foreign bank accounts.

The accused also allegedly made reward payments to US citizens and paid hosting fees to Carpathia and Cogent via similar services.

4. Could this precedent extend to other cloud services?

If data or transactions made on a server based in the United States are found to be a business activity that brings corporations and their employees under U.S. jurisdiction, the Megaupload case could have significant consequences for international users of US-based cloud computing services such as Microsoft Azure, Amazon Web Services, Rackspace or Google AppEngine.

It would equally concern users of online storage services, such as DropBox or Mozy, even users of Apple's iCloud service. Users of the former could lose significant troves of company data should their sites ever be shut down as Megaupload has.

The U.S. Department of Justice didn't hold any punches in this regard, noting that the case "directly targets the misuse of a public content storage and distribution site to commit and facilitate intellectual property crime."

Vincent said cloud service users should be concerned that the "basis for the US Government asserting jurisdiction on this matter is that servers were based in Virginia in the United States."

Copyright applies.

http://mobile.itnews.com.au/Article.aspx?CIID=287823&type=News

---