Megaupload

the

Copyright Lobby

and the

Future of Digital Rights

The **United States** *vs* **You** (and **Kim Dotcom**)

A White Paper by
Robert R. Amsterdam and Ira P. Rothken

> *The United States Congress [...] is now incapable of passing laws without permission from the corporate lobbies and other special interests that control their campaign finances.*
>
> **Al Gore**
> Former Vice President of the United States [1]

> *Viewed up close, copyright bears little resemblance to the kinds of property that conservatives value. Instead, it looks like a constantly expanding government program run for the benefit of a noisy, well-organized interest group.*
>
> **Stewart Baker**
> Former Assistant Secretary for Policy at the
> Department of Homeland Security, under President George W. Bush [2]

> *Those who count on quote 'Hollywood' for support need to understand that this industry is watching very carefully who's going to stand up for them when their job is at stake. Don't ask me to write a check for you when you think your job is at risk and then don't pay any attention to me when my job is at stake.*
>
> **- Chris Dodd**
> Chairman of the Motion Picture Association of America and
> Former Senator of the United States [3]

Executive Summary

The criminal prosecution of Megaupload and Kim Dotcom is purportedly the ***"largest copyright case in history,"*** involving tens of millions of users around the world, and yet it is founded on highly dubious legal principles and apparently propelled by the White House's desire to mollify the motion picture industry in exchange for campaign contributions and political support.

The U.S. government's attack on the popular cloud storage service Megaupload and the dramatized arrest of Kim Dotcom, the company's principal founder – together with the seizure of all their worldwide assets – represents one of the clearest examples of prosecutorial overreach in recent history. One day after the U.S. Congress failed to enact the controversial Stop Online Piracy Act (SOPA), the executive branch of the U.S. government commandeered Megaupload in a coordinated

[1] ***"The Future: Six Drivers of Global Change,"*** by Al Gore, Random House, 2013.

[2] Mr. Baker's quote was first published in the Wall Street Journal in 2004. The excerpt is cited by the author in a blog post here: http://www.volokh.com/2010/11/20/girl-talk-and-intellectual-property/

[3] ***"Hollywood Lobbyist Threatens to Cut Off Obama,"*** Fox News, January 19, 2012 (http://www.foxnews.com/politics/2012/01/19/exclusive-hollywood-lobbyist-threatens-to-cut-off-obama-2012-money-over-anti/)

global take-down, and drew battle lines between digital rights advocates, technology innovators and ordinary information consumers on the one side, and Hollywood and the rest of the Copyright Lobby on the other.

Megaupload operated for seven years as a successful cloud storage business that enabled tens of millions of users around the world to upload and download content of the users' own choosing and initiative. The spectrum of content ran from (to name just a few) family photos, artistic designs, business archives, academic coursework, legitimately purchased files, videos and music, and – as with any other cloud storage service – some potentially infringing material. Despite Megaupload's lawful uses, the U.S. government has charged the company and its executives under the Racketeer Influenced and Corrupt Organizations (RICO) Act, and has branded the company, its personnel and its tens of millions of users a "criminal enterprise" dedicated solely to infringing U.S. copyright laws.

The U.S. government's case against Megaupload is grounded in a theory of criminal secondary copyright infringement. In other words, the prosecution seeks to hold Megaupload and its executives criminally responsible for alleged infringement by the company's third-party cloud storage users. The problem with the theory, however, is that secondary copyright infringement is not – nor has it ever been – a crime in the United States. The federal courts lack any power to criminalize secondary copyright infringement; the U.S. Congress alone has such authority, and it has not done so.

As such, the Megaupload prosecution is not only baseless, it is unprecedented. Although the U.S. government has previously shut down foreign websites engaged in direct infringement, such as the sale or distribution of infringing material, never before has it brought criminal charges against a cloud file storage service because of the conduct of its users. Thus, the Megaupload case is the first time the government has taken down a foreign website – destroying the company and seizing all of the assets of its owners (and the data of its users), without so much as a hearing – based on a crime that does not exist.

To make matters worse, in order to persuade other countries to cooperate with the take-down, the U.S. government misled them into believing that Megaupload was involved in direct infringement. One of many such examples involved applications for warrants to search and seize Megaupload computer servers in Canada. In those applications, the U.S. government misled the Canadian authorities by stating that the U.S. was prosecuting Megaupload for operating and administering websites that "reproduce and distribute" infringing material. Even if the U.S. government had believed Megaupload was reproducing and distributing infringing material (which it was not), the government was certainly aware that the criminal charges it was prosecuting were not based on any such allegations. Further, the U.S. government made those misrepresentations to Canadian authorities without any advance notice to Megaupload, meaning that nobody was present to refute them.

Even if the U.S. government's wishful expansion of the criminal copyright law into the realm of secondary infringement were tenable (which it is not), Megaupload is shielded from criminal liability by specific "safe harbor" provisions in the Digital Millennium Copyright Act (DMCA), included in the law to protect companies like Megaupload that make efforts to remove infringing material in response to "take- down" notices issued by copyright holders. The DMCA's safe harbor provisions have been upheld repeatedly by the federal courts, most recently in the Southern District of New York in Viacom v. YouTube, which (among other things) determined that mere generalized knowledge of infringement does not deprive a service provider of the protections of the DMCA's safe harbor provisions. [4]

On April 18, 2013, the Viacom court rejected the argument that YouTube was only entitled to safe harbor protection if it could prove that it was unaware of infringement. The court noted that service providers serve a useful function, and pointed out that given the volume of content being uploaded/ downloaded on a site like YouTube, "no service provider could possibly be aware of the contents of each such video." [5] Congress put the burden on the copyright owner to notify the service provider of infringements – in writing and with specified contents – and the court concluded that the burden could not be shifted back to YouTube to disprove its knowledge. YouTube was entitled the DMCA's safe harbor provisions because Viacom was not able to prove that YouTube had actual knowledge of specific acts of infringement.

The Viacom court also emphasized that the benefits of DMCA safe harbor protection did not require affirmative monitoring by YouTube based on some general awareness that infringement may be occurring. Nothing in the DMCA required YouTube to affirmatively seek out facts indicating infringing activity. Even though YouTube could potentially locate infringements using its own identification tools, it had no duty under the DMCA to do so.

The Court stated that "the governing principle must remain clear: knowledge of the prevalence of infringing activity, and welcoming it, does not itself forfeit the safe harbor." [6]

While Megaupload systematically responded to countless DMCA take-down notices, it went even further to guard against copyright violations. It voluntarily gave major copyright holders direct access to its servers to remove links they considered to be infringing – without any oversight by Megaupload – and without requiring them to follow statutory take-down notice procedures.

[4] See Viacom Int'l, Inc. v. Youtube, Inc., 2013 U.S. Dist. LEXIS 56646 (S.D.N.Y. Apr. 18, 2013).

[5] Id., at 8.

[6] Id., at 19.

The U.S. government's case is legally untenable for the additional reason that Megaupload and its executives do not reside in the United States and most of the company's activities occurred outside the United States. The government is foreclosed from prosecuting Megaupload in the Eastern District of Virginia (or anywhere in the United States) because the court lacks jurisdiction over the company. More specifically, the prosecution is unable to serve Megaupload with criminal service of process – which, in the case of a corporate entity, calls for service of a summons – because the company has neither an agent nor an office inside the United States. Although the government has advanced a number of arguments why it should be allowed to bypass due process and skirt the express requirements of the Federal Rules of Criminal Procedure, none of its arguments has any basis in law.

Nevertheless, despite these glaring obstacles, the U.S. government sought and obtained a criminal indictment against Megaupload, seized all of the global assets of the company and its founders, including domain names, and forced the company into extinction. The seizure order was requested ex parte, which is to say that Megaupload was given no notice and was not present at the hearing to object to the government's request. And because the U.S. government has not attempted to serve Megaupload with a summons (and it cannot, due to lack of jurisdiction), the seizure order is in a sort of legal limbo; it remains in place yet, as a practical matter, Megaupload cannot challenge it, even now, more than a year later.

Meanwhile, Megaupload's servers – which contain petabytes of important evidence relevant to the defense – have been taken offline for lack of funding. Astonishingly, the U.S. government initially was content to let the data on the servers be destroyed, and although that has not occurred, the equipment has been gathering dust for many months and is in danger of deteriorating. The U.S. government will not agree to release a single penny of Megaupload funds to allow for consumers to get access to their data, or to preserve the evidence, or even to mount a legal defense in the United States.

Those are not the only dirty tactics the U.S. government has employed to try to manufacture a criminal case against Megaupload. The government violated its legal obligations by misrepresenting facts and intentionally omitting critical, exculpatory information when it applied for the search warrants to seize Megaupload's domain names.

Specifically, the government's warrant applications said that Megaupload had been informed about 39 infringing copies of copyrighted motion pictures yet had neglected to remove them from its servers, thereby suggesting that Megaupload possessed a criminal state of mind, a necessary element for the warrants to issue. In actuality, the FBI had informed Megaupload – through Carpathia Hosting, one of the company's server vendors, which the government had deputized to communicate on its behalf – that the FBI was conducting an investigation into those files.

In support of its application for a warrant, the FBI agent stated under oath:

> *Since the investigation is continuing, the Affiant requests that this search warrant affidavit be sealed until such time as the Court directs otherwise. Disclosure of the search warrant affidavit at this time would seriously jeopardize the ongoing investigation, as such disclosure may provide an opportunity to destroy evidence, change patterns of behavior, notify confederates, or allow confederates to fee or continue flight from prosecution. Notwithstanding the above, the government requests that Carpathia and its customer MegaUpload be permitted to view the warrant and Attachments A and B to the warrant to assist them in executing the warrant.* [7]

Thus, through Carpathia, the FBI provided Megaupload with a copy of a sealed warrant concerning alleged third-party infringement and asked the company to treat the warrant with utmost secrecy, suggesting that any action by Megaupload to take down the materials might alert the infringing third parties and jeopardize the ongoing investigation. Naturally, Megaupload cooperated and preserved the status quo so that the FBI's investigation could proceed unhindered.

Thus, the U.S. government manipulated Megaupload to leave certain materials in place (while failing to inform Megaupload it was itself a target of the investigation), then twisted the facts and used Megaupload's cooperation as the only direct evidence of purported criminal intent. At the same time, prosecutors intentionally omitted all mention of numerous anti-piracy measures Megaupload had long since put in place to deter infringement by its users, all of which demonstrate an absence of criminal intent. Based on those tandem due process violations – mischaracterization of facts, coupled with the omission of exculpatory evidence, neither of which could be argued by a defendant who was not present – the government secured its search warrants, seized Megaupload's domain names, and in an instant effectively destroyed the company.

In New Zealand, Kim Dotcom – one of Megaupload's founders and a resident of that country – now faces extradition proceedings initiated by the U.S. government. There, a New Zealand government

[7] See ***"Megaupload Assisted U.S. Prosecution of Smaller File-Sharing Service"*** Wired, Oct. 18, 2012, http://www.wired.com/threatlevel/2012/11/megaupload-investigation-roots/, which includes a link to the search warrant and supporting affidavit, http://www.wired.com/images_blogs/threatlevel/2013/12/Carpathia-search-warrant.pdf

intelligence arm was persuaded to spy illegally on Kim Dotcom. Those due process abuses were eventually brought to light in court proceedings, forcing New Zealand's Prime Minister to issue a public apology.[8] Further, when the New Zealand authorities raided Kim Dotcom's home in January 2012, they did so based on search warrants that a New Zealand court later determined to be illegal.

Additionally, the New Zealand court determined that the U.S. government had transferred Kim Dotcom's and the other Megaupload executives' hard drive data out of New Zealand in violation of New Zealand law. To date, the U.S. authorities have refused to return the data, despite the fact that they were acquired illegally and in violation of Kim Dotcom's privacy rights, and notwithstanding their importance to any defense against the criminal charges.

Under ordinary circumstances, there would be no reason for illegal surveillance, a 72-page indictment, a RICO "Mega Conspiracy" label, an overly expansive and unsupported legal theory of criminal liability, a dramatic raid on a private residence, an abrupt seizure of hundreds of millions of private computer files, willful omission of exculpatory evidence and other due process violations, a worldwide seizure of the defendants' assets without any allowance for defense costs, and a black media campaign with an inordinate focus on the principal founder's financial success and flamboyant lifestyle. Those variables, among other abuses, make sense only in the context of some motivating factor outside the U.S. Department of Justice's mandate. Indeed, the outside motivating factor in this case stems from Motion Picture Association of America's (erroneous) view of Megaupload as "the very top of the piracy pyramid,"[9] coupled with the current Administration's desire to placate an association whose members, as a group, are some of the Democratic Party's strongest political supporters and most generous campaign contributors.

There is little dispute that the prosecution of Megaupload and Kim Dotcom has been driven principally by the Motion Picture Association of America (MPAA). The MPAA – which represents the six largest film and television production studios in Hollywood – publicly labeled Megaupload a "notorious market outside of the United States" in a November 2010 submission to the Office of the U.S. Trade Representative's (USTR).[10] Behind the scenes, however, the MPAA had already persuaded the FBI to initiate an investigation into Megaupload's business months before.[11]

[8] See http://www.telegraph.co.uk/technology/internet/9569986/Kim-Dotcom-NZ-Prime-Minister-apologises-over-unlawful-spy-operation.html.

[9] See http://news.cnet.com/8301-31001_3-57369825-261/nobody-wanted-megaupload-busted-more-than-mpaa/.

[10] See http://www.mpaa.org/resources/fdff7027-1a9e-46dc-9a80-7cf20aa1b686.pdf, at 5.

[11] See http://news.cnet.com/8301-31001_3-57369825-261/nobody-wanted-megaupload-busted-more-than-mpaa/ (MPAA referred Megaupload and Kim Dotcom to law enforcement in early 2010).

In early 2011, at or around the time U.S. Senator Chris Dodd took over as Chairman and CEO, the MPAA boosted its already robust Washington lobbying activity. Based on mandatory public disclosures, the MPAA's agenda appears to have included pushing the proposed SOPA bill and its Senate corollary the Protect IP Act (PIPA) – both of which were aimed at foreign websites heretofore beyond the reach of the U.S. courts – and making an example of Megaupload. The MPAA's lobbyists met with Vice President Joseph Biden, a former Senate colleague and political ally of Chris Dodd, to whom the Vice President had referred only months earlier as "one of my best friends in life." [12] The MPAA also took the unusual step of lobbying U.S. law enforcement agencies directly, including the Department of Justice, the FBI and the Department of Homeland Security, all of which would later play direct roles in the investigation, arrest, seizure and prosecution of Megaupload and Kim Dotcom.

In certain significant ways, the MPAA's support for SOPA is also reflected in the U.S. government's legal theories against Megaupload. SOPA would have permitted copyright holders to make use of the U.S. federal courts to require Internet service providers to block their subscribers' access to domain names of alleged "foreign infringing sites," and bar search engines, payment processors and advertisers from doing business with such foreign sites. [13] Notably, SOPA would have defined an "infringing foreign site" as any site "committing or facilitating" copyright infringement, regardless of whether the site was – like Megaupload – engaged in significant non-infringing uses.

SOPA and PIPA were widely opposed on a variety of grounds, including internet security concerns, First Amendment issues and due process considerations, among others. When the White House released a public statement in January 2011 expressing the view that any legislation should reflect the interests of not only content creators but also the technology sector, Chris Dodd made a Fox News appearance on behalf of the MPAA and issued a direct threat to the Obama Administration and its reelection campaign:

> *I would caution people don't make the assumption that because the quote "Hollywood community" has been historically supportive of Democrats, which they have, don't make the false assumption this year that because we did it in years past, we will do it this year.* [14]

[12] See http://www.cbsnews.com/8301-503544_162-12005-503544.html.

[13] Originally, both SOPA and its U.S. Senate corollary – the Protect IP Act (PIPA) –contained Internet service provider site blocking provisions, but opposition was so strong that subsequent versions of the bills omitted those provisions.

[14] See http://www.foxnews.com/politics/2012/01/19/exclusive-hollywood-lobby-ist-threatens-to-cut-off-obama-2012-money-over-anti/.

Campaign contributions speak loud and clear in Washington, and the required quid pro quo, concealed in this instance by the barest of fig leaves, was unmistakable. Although SOPA was ultimately defeated, the MPAA's bare-knuckle tactics explain much about the U.S. government's conduct in the Megaupload case. It is no coincidence, for example, that the indictment was issued out of the Eastern District of Virginia, where Neil MacBride – formerly Chief Counsel to then Senator Joseph Biden on the Senate Judiciary Committee – is the United States Attorney. It is also noteworthy that the MPAA achieved through the U.S. Department of Justice's attack on Megaupload at least as much as it would have accomplished against foreign websites had SOPA passed.

Professor Goldman described the dynamic precisely:

> *[T]he government's prosecution of Megaupload demonstrates the implications of the government acting as a proxy for private commercial interests. The government is using its enforcement powers to accomplish what most copyright owners haven't been willing to do in civil court (i.e., sue Megaupload for infringement); and the government is doing so by using its incredibly powerful discovery and enforcement tools that vastly exceed the tools available in civil enforcement; and the government's bringing the prosecution in part because of the revolving door between government and the content industry (where some of the decision-makers green-lighting the enforcement action probably worked shoulder-to-shoulder with the copyright owners making the request) plus the Obama administration's desire to curry continued favor and campaign contributions from well-heeled sources.* [15]

The degree to which the Copyright Lobby, and the MPAA specifically, have managed to instrumentalize the current Administration to take down a foreign corporation and its executives is, quite literally, un-American. There was a time, not very long ago, when the United States stood for principled standards and the Rule of Law. In years past, the kind of open influence peddling by the MPAA's Chris Dodd during a hotly contested presidential reelection campaign would have drawn condemnation from all quarters. But those values appear to have fallen by the wayside under this White House, which seems content to violate the due process rights of criminal defendants, mislead the courts, and advance baseless legal theories so long as its fund raising remains uninterrupted.

The MPAA's overt use of campaign contributions to sway the U.S. government into engaging in what

[15] See http://blog.ericgoldman.org/archives/2012/04/megaupload.htm

amounts to unlawful action against Megaupload reflects a form of State Capture, a term coined by the World Bank to describe a brand of corruption characterized by the ability of a relatively small number of private interests to shape the official rules of the game through direct payments or other forms of financial influence. By threatening to revoke vital political and monetary support from the Administration at a crucial moment, the MPAA has exercised de facto control over key levers of executive power in Washington – law enforcement, prosecutors, trade negotiators – and is using those instruments of state power to further the financial interests of its members in Hollywood. For example:

- Section 181 of the Internal Revenue Code, known as the "Domestic Film Production Incentive Program," gives television studios steep tax deductions on full or partial costs of their productions on a per-episode basis. In 2013, Congress retroactively extended that tax break to 2012. [16]

- MPAA member studios receive a tax break in the order of $1.51 billion every year in the form of subsidies or incentives from individual state governments, allowing them to defray income and/or sales taxes incurred during filming in those states. [17]

- The Copyright Lobby is able to access the U.S. legislative drafting process. For example, Michael O'Leary, the MPAA's Senior Executive Vice President for Global Policy and External Affairs, confirmed that the MPAA was responsible for the language contained in the SOPA bill. [18]

- The Copyright Lobby is able to access and utilize the U.S. diplomatic apparatus to pressure other countries to enact legislation that benefits the Copyright Lobby. In Spain, for example, the MPAA lobbied for passage of a new copyright law known as "Ley Sinde," which allows copyright holders to discovery the identity of alleged infringers and block their websites within 48 hours.

- The Copyright Lobby facilitated development of the Special 301 "blacklist" of the

[16] See ***"Fiscal Cliff: Hollywood Tax Incentives Renewed Under Deal,"*** Hollywood Reporter, Jan. 2, 2013 (http://www.hollywoodreporter.com/news/fiscal-cliff-hollywood-tax-incentives-407442)

[17] GAI Report: ***"Let the Credits Roll: An Examination of the Tax Film Subsidy System,"*** Feb. 13, 2013 (http://g-a-i.org/gai-report-let-the-creditsroll-an-examination-of-the-tax-film-subsidy-system/)

[18] See http://mediadecoder.blogs.nytimes.com/2011/11/30/expect-some-toning-down-of-antipiracy-bills-says-movie-industry-supporter/.

Office of the United States Trade Representative (USTR), which gives negotiating leverage to the USTR over foreign governments to persuade them to take action against alleged infringers in their countries. [19]

- The Copyright Lobby has been able to work closely with U.S. trade officials to insert favorable language into various trade agreements. For example, the MPAA was active in negotiating the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) of the World Trade Organization (WTO), which (among other things) now includes remuneration for royalty payments to corporations. The MPAA's involvement in the TRIPS negotiations marked an increase in private sector lobbying in the international system, making it virtually impossible to interpret TRIPS provisions without input from the private sector, and ensuring an ongoing influential role for the MPAA in future enforcement of TRIPS provisions with regard to movie copyrights. [20] The MPAA was also involved in drafting the failed Anti-Counterfeiting Trade Agreement and the Trans-Pacific Partnership Agreement, which is presently in the negotiation phase.

Unfortunately, as a consequence of its complicity in the arrangement, this White House has abdicated the moral high ground (if it ever held it) from where it might credibly exhort other countries to abide by the Rule of Law as a governing principle in all circumstances.

The U.S. government's attack against Megaupload bears all the hallmarks of a contract prosecution: a case resting on erroneous theories of criminal law, littered with due process violations and prosecutorial abuses, carried out for the benefit of a select few in exchange for their political and financial support. In the name of eliminating copyright infringement, Hollywood has exerted a corrupting influence in Washington, leading us all down a slippery slope that not only threatens innovation and Internet freedom, but also has profound implications for constitutional principles of free speech, privacy and due process. Megaupload and Kim Dotcom are today's targets, but the crosshairs can just as easily be trained on anybody who dares challenge or inconvenience a special interest that holds sway in Washington, and the current Administration – with its notoriously insatiable appetite for campaign contributions – seems all too willing to cooperate.

[19] See http://www.elpais.com/articulo/espana/EE/UU/ejecuto/plan/conseguir/ley/antidescargas/elpepuesp/20101203elpepunac_52/Tes.

[20] Kevin Lee, ***"The Little State Department"***: Hollywood and the MPAA's Influence on U.S. Trade Relations, 28 Nw. J. Int'l L. & Bus. 371 (2007-2008).

The unfortunate case of Aaron Swartz also comes to mind. Swartz was a young internet entrepreneur – founder of Infogami and co-founder of Reddit and RSS co- developer – an activist for government reform, digital rights and civil liberties, and a vocal opponent of SOPA. He was indicted in 2011 for allegedly attaching a laptop to MIT's computer network and downloading a large number of articles from an archive of academic journals. The prosecution alleged that Swartz intended to make the papers available on P2P file-sharing sites. [21]

Tragically, Aaron Swartz killed himself on January 11, 2013, about two weeks before a significant evidence suppression hearing in his legal case. Shortly after Swartz's death, his attorney sent a letter to the Office of Professional Responsibility of the U.S. Department of Justice, requesting an inquiry into the conduct of the lead prosecutor, Assistant U.S. Attorney Stephen Heymann. According to Swartz's lawyer:

> *. . . AUSA Heymann appears to have failed timely to disclose exculpatory evidence relevant to Mr. Swartz's pending motion to suppress. Indeed, evidence suggests AUSA Heymann may have misrepresented to the Court the extent of the federal government's involvement in the investigation into Mr. Swartz's conduct prior to the application for certain search warrants. Second, AUSA Heymann appears to have abused his discretion when he attempted to coerce Mr. Swartz into foregoing his right to a trial by pleading guilty. Specifically, AUSA Heymann offered Mr. Swartz four to six months in prison for a guilty plea, while threatening to seek over seven years in prison if Mr. Swartz chose to go to trial.* [22]

While the factual similarities between the Aaron Swartz's prosecution and the Megaupload matter are purely tangential, both cases evoke a common theme of prosecutorial abuse in matters touching upon copyright.

On April 25, 2013, Article 19 – a non-governmental organization dedicated to defending the right to freedom of expression – published The Right to Share: Principles of Freedom of Expression and Copyright in the Digital Age. There, it states that:

[21] See http://en.wikipedia.org/wiki/Aaron_Swartz.

[22] See http://big.assets.huffingtonpost.com/HeymannOPRletter.pdf.

> *The Principles were developed as a result of concerns that the fundamental human right to Freedom of Expression, guaranteed in UN and regional human rights instruments and nearly every national constitution, has been increasingly eroded on the grounds of protecting copyright. The Internet has been at the centre of an alarming expansion of copyright claims at the expense of freedom of expression and, more generally, the protection of human rights. These principles affirm that the right to freedom of expression and the free flow of information and ideas cannot be seen as marginal to such developments.* [23]

Section 1.4 of the Article 19 principles provides that:

> *No restriction on freedom of expression on the ground of protection of the rights of others, including copyright, may be imposed unless the State can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect those interests. The burden of demonstrating the validity of the restriction rests with the State.*
>
> ***
>
> *(d) A restriction on freedom of expression is proportionate in a democratic society only if:*
>
> ***I.*** *It is the least restrictive means available for protecting that interest; and*
>
> ***II.*** *The restriction is compatible with democratic principles.* [24]

From a human rights perspective, the attack on Megaupload lacks all sense of proportion and therefore violates the fundamental rights of the company and its executives. Additionally, the U.S. government's numerous due process violations infringe upon internationally guaranteed human rights.

In this digital age, with ever-expanding theories of criminal liability for infringement, the U.S. government's target could be virtually anybody; we are all at risk. This is the Megaupload story, and it impacts you directly.

[23] See http://www.article19.org/resources.php/resource/3716/en/.

[24] See http://www.article19.org/data/files/medialibrary/3716/13-04-23-right-to-share-EN.pdf.

1 A Raid Made in Hollywood

COATESVILLE, NEW ZEALAND
20 JANUARY 2012, 06:46:

The early morning air was shattered by the thumping rotors of helicopters swooping down, seemingly out of nowhere, onto the grounds of a sprawling private residence. Dozens of units of New Zealand's elite Special Tactics Group and Armed Offenders Squad, dressed in body armor and operating under the direction of the FBI, fanned out across the property, taking up tactical positions and disabling security personnel. Armed with M4 semi-automatic rifles and trained attack dogs, a total of some 70 men swarmed the premises. With an overwhelming show of force, they smashed down doors, breached the property, neutralized its occupants and successfully detained their targets.

By all appearances, the FBI was in hot pursuit of a fugitive drug lord or a deadly terrorist cell. A surprise daybreak operation of that scale would surely indicate genuine concern that armed and dangerous criminals might be lurking inside, poised for a showdown, holed up and ready for a shoot-out with authorities.

But in fact it was nothing of the sort. The man who lives in that home in the serene, pastoral community of Coatesville, New Zealand is much more dangerous. He is a successful Internet entrepreneur – the founder of Megaupload, one of the world's most popular cloud storage services – and he has angered the Motion Picture Association of America. Some users of the Megaupload service had stored movie files in violation of U.S. copyright laws, and the White House was eager to appease its Hollywood benefactors, who wanted to make an example of Megaupload.

By the time the raid was over, Kim Dotcom and three other Megaupload executives – Finn Batato, Mathias Ortmann and Bram van der Kolk – were behind bars. Kim Dotcom had been forcibly extracted from a safe room in the compound, where he had fled in alarm, assuming criminals had invaded the home. "I had a punch to the face, I had boots kicking me down to the floor, I had a knee into the ribs, then my hands were on the floor, one man was standing on my hand," he later told the Auckland High Court under cross-examination. [25] His wife, 27-weeks pregnant with twins at the time, was so traumatized that she was taken to the hospital with pain and cramping.

Hours before launching the raid, aptly dubbed "Operation Debut," federal prosecutors in the United States tipped off journalists with the anticipated highlights of the operation. Hundreds of

[25] http://www.3news.co.nz/VIDEO-What-really-happened-in-the-Dotcom-raid/tabid/817/articleID/264651/Default.aspx

computer servers around the world would soon be shut down. The domain names of Megaupload and its related websites would all be seized and emblazoned with the FBI seal for the world to see. No matter that millions of innocent users would lose non-infringing personal files stored on the Megaupload servers. The important thing was that the company – which at one point accounted for 4% of the entire world's Internet traffic – would be destroyed in an instant.

When the operation was over, the U.S. Department of Justice issued a press release: "This action is among the largest criminal copyright cases ever brought by the United States and directly targets the misuse of a public content storage and distribution site to commit and facilitate intellectual property crime." [26]

A 72-page grand jury indictment was soon released, filed in secret in a Virginia federal court two weeks before the raid. It stated that Megaupload, Kim Dotcom and six other Megaupload executives were criminally responsible for any and all copyright infringement by the company's customers. Megaupload and the six executives were labeled criminal racketeers – charged, like the Gambino crime family, under the Racketeering Influenced and Corrupt Organizations (RICO) Act enacted to combat organized crime – accused of having formed Megaupload for the sole purpose of operating a "worldwide criminal organization," an ongoing conspiracy to commit secondary copyright infringement.

Yet branding Megaupload and its executives as criminals was not enough. U.S. prosecutors applied to a federal court in Virginia, behind closed doors, for an order allowing the government to seize all worldwide assets belonging to Megaupload, Kim Dotcom and the other defendants – including those of unindicted third parties, such as the defendants' wives and Kim Dotcom's personal assistants – depriving the defendants of any financial resources with which to fund a defense or counter the charges. The U.S. government promptly initiated extradition proceedings to bring Kim Dotcom to the United States to stand trial. Eventually, after 31 days behind bars, he was released on bail in New Zealand, against the wishes of the U.S. government. [27]

Meanwhile, luxury vehicles owned by Kim Dotcom were paraded in front of television cameras, while the media published detailed lists of seized properties comprising some $67 million in assets.

Over the years, the content industry has worked to create a link between copyright infringement and piracy, gaining a subtle upper hand simply by shaping the phraseology:

[26] ***"Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement,"*** Department of Justice website, Jan. 19 , 2012 (http://www.justice.gov/opa/pr/2012/January/12-crm-074.html).

[27] ***"Kim Dotcom Wins Bail in Fight against U.S. Extradition,"*** Reuters, Feb. 22, 2012 http://newsandinsight.thomsonreuters.com/Legal/News/2012/02_-_February/Kim_Dotcom_wins_bail_in_fight_against_U_S__extradition/.

> *Piracy remains a powerfully evaluative word. To be called an intellectual property pirate is to be condemned. In a world where attention spans are divided by the media into ten-second sound bites it is the perfect word to use on TV, videocassettes, newspaper headlines, and the radio. The received folk memory of "pyrates and rovers" on the sea does the rest.* [28]

Copyright holders have been so successful at linking "infringement" with "piracy" that the two words have become virtually interchangeable. Even the Special 301 Reports issued annually by the Office of the United States Trade Representative (USTR) speak of copyright "piracy." [29] In the specific case of Megaupload and Kim Dotcom, the MPAA first labeled them pirates in November 2010 in response to the USTR's request for information on markets "where counterfeit and pirated products are prevalent . . .."[30]

And so Hollywood had cast its latest villain: Kim Dotcom and his gang were now "pirates" reveling in illicit spoils, no longer innovative Internet entrepreneurs, but thieves.

2 The Rise of Megaupload and Cloud Computing

Kim Dotcom was born Kim Schmitz on January 21, 1974 in Kiel, Germany. Brilliant from a young age, he struggled with boredom in school and became known for clowning in class. At the age of 12, his life changed forever when his mother bought him his first computer and he quickly immersed himself in the world of software coding and computer gaming. He mastered games, and even designed some games of his own for sale. Before long, he was able to generate enough income from his computing skills to rent a small apartment for himself.

Like many technology gurus before him – Steve Jobs and Steve Wozniak, to name two prominent

[28] ***"Information Feudalism: Who Owns the Knowledge Economy?"*** by Peter Drahos and John Braithwaite (The New Press: 2007, pp. 29).

[29] See http://www.ustr.gov/about-us/press-office/reports-and-publications/2013/2013-special-301-report.

[30] See http://www.mpaa.org/resources/fdff7027-1a9e-46dc-9a80-7cf20aa1b686.pdf, at 3.

examples – Kim initially gained fame as a teenage hacker. [31] He ran his own bulletin board system (BBS) from a modem array, and he experimented with X.25 networks, PBX phone networks and "blue boxing." He met Mathias Ortmann, who would later become his business partner and Megaupload's Chief Technology Officer.

Kim converted his hacking skills into a business enterprise by launching a data security consulting firm with Mathias Ortmann they named Data Protect. It was one of the world's first "white hat" security consultancies, serving such corporate giants as Daimler and the German stock exchange Deutsche Boerse, by auditing and ensuring the security of their networks. [32]

Over the next four years, Data Protect grew to some 30 employees, with annual revenues of several million dollars. Kim, however, was frustrated by what he saw as growth limitations in the consulting sector. He sold Data Protect to a competitor in 2001 and went on to pursue start-up investment opportunities in the booming tech sector.

In 2004, Kim moved to Hong Kong, where he began to focus on a solution to a problem he had stumbled upon almost by accident. As an amateur auto-racing enthusiast, he had tried to email his personal racing videos to friends, only to have the emails rejected because his video files were too large. Kim set out to innovate a solution and, after months of work, his developers constructed a website and a series of servers that could efficiently store and transfer files too large to transmit as email attachments. Megaupload was thus born, and was launched to the public in 2005.

Megaupload served a growing demand for users to access their personal files from any computer in the world, allowing them to break free from their former reliance on their own computer hard drives to store and backup data. Instead, customers could upload, download, use and share whatever content they selected – family photos, financial records, collaborative business documents, academic materials, video and music files (to name just a few) – hosting their files on the Megaupload servers, in a "cloud" of sorts, and reach them at will from any computer with access to the Internet.

Cloud computing offers a variety of benefits, including broad network access, resource pooling, rapid

[31] For more information on the early hacking careers of Jobs and Wozniak, see ***"Phreaks and Geeks,"*** Slate.com, Feb. 1, 2013 (http://www.slate.com/articles/technology/books/2013/02/steve_jobs_and_phone_hacking_exploding_the_phone_by_phil_lapsley_reviewed.html).

[32] ***"Inside the Mansion—and Mind— of Kim Dotcom, the Most Wanted Man on the Net,"*** Wired, Oct. 18, 2012 (http://www.wired.com/threatlevel/2012/10/ff-kim-dotcom/all/).

elasticity, on-demand self-service, and measured, cost-effective service. [33] Megaupload's primary business, Megaupload.com, was a commercial website that offered a popular Internet-based storage platform for customers, ranging from individuals to large businesses. Its storage platform allowed users to store files in the Internet "cloud" and use online storage space and bandwidth as needed.

In a crowded field of competitors offering cloud storage services, Megaupload quickly established itself as a market leader. Megaupload was fast, free and easy to use. When Megaupload was shut down, the content stored across its servers spanned a veritable ocean of accumulated human learning, knowledge, information, personal narrative, artistry and entertainment. At one point in its history, Megaupload.com was estimated to be the 13th most frequently visited website on the entire Internet. The site had more than one billion unique visitors per year, more than 60 million registered users, and an average of some 50 million daily visits. It accounted for, on average, approximately 4% of the total traffic across the Internet.

In order to host the massive amount of unique data uploaded by its users, Megaupload leased thousands of computer servers all over the world, most of them outside the United States. Megaupload's income was derived primarily from two sources: premium subscriptions and online advertising. Premium subscriptions could be purchased online for as little as a few dollars per day or as much as $260 for a lifetime. In exchange for payment of the subscription fee, premium users enjoyed more storage space, higher transfer speeds and additional site features. Subscription fees collected during the company's existence were estimated to exceed $150 million, whereas receipts from online advertising on Megaupload.com and affiliated sites totaled a mere fraction of that, estimated at somewhere above $25 million.

Although Megaupload was a market leader, the technology it employed was not unique amongst cloud storage service providers. Like other providers – Dropbox, for example – Megaupload optimized cloud storage with "hash" technology. Whenever a file was uploaded to the site, an automated system used a mathematical algorithm to calculate a unique identifier, called an "MD5 hash," for the file. If the system determined that multiple users had uploaded the identical file, Megaupload would retain only one instance of the file, and generate a unique link for each individual user, called a Uniform Resource Locator or URL. One user might choose to keep their unique link private; another user might wish to share their link with a close friend or family member by way of an e-mail; and yet another user might make it more widely available by embedding it in a webpage. Megaupload simply stored users' files on its servers at the request of users. Thus, contrary to what

[33] Peter Mell & Timothy Grance, ***The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*** at 2, NIST Special Publication 800-145 (Sept. 2011).

the U.S. government has suggested in its indictment, Megaupload's core business model was no different from numerous other mainstream Internet service providers.

3 A Case of Fatal Flaws

The case against Megaupload and its executives is extraordinary, but not because – in the words of the U.S. Department of Justice – it is "the biggest copyright case in history." The case is astonishing because it is so clearly meritless. It is marked by layer upon layer of flawed legal reasoning, by repeated prosecutorial abuses and due process violations, and by the corrupting influence of lobbyists' fees and campaign contributions. It is clearly not the biggest copyright case in history, but it may be the most scandalous, and it signals an ominous future for network technology, innovation and free speech.

Criminal copyright infringement requires willful infringement – a very rigorous level of criminal intent – and it is one of the rare criminal claims where both ignorance of the law and a defendant's mistaken belief that he is compliant with the law are complete defenses. Megaupload immediately responded to take-down notices from copyright holders on millions of occasions. The company's subjective belief that it was operating within the law (even if it turns out to have somehow been wrong in that regard) should by itself be enough to negate the criminal willfulness requirement, especially considering the novel nature of the prosecution's legal theory.

a. No Criminal Liability for Secondary Copyright Infringement

The U.S. government argues that Megaupload and its executives encouraged criminal copyright infringement by the company's users, and should therefore be held criminally responsible for the infringing conduct of those third parties. Gordon Campbell's article in the Kiwi publication Werewolf highlights the implications of that approach: "As an offence, 'criminal contributory copyright infringement' sounds like trying to prosecute the president of a gun club for 'contributory bank robbery' because some club members used their pistols to rob Wells Fargo." [34] But the government's problem is not merely the slippery slope it starts down when it tries to hold companies responsible for

[34] ***"The Show (and Tell) Trial,"*** Werewolf, March 27, 2013 (http://werewolf.co.nz/2013/03/the-show-and-tell-trial/).

the conduct of their customers; the prosecution's legal theory has very real – indeed, insurmountable – hurdles as well.

The fact of the matter is that the notion of criminal liability for secondary copyright infringement does not exist in U.S. law. The attempt by prosecutors to expand criminal liability for secondary infringement by couching it as "aiding and abetting" or "conspiracy" goes against established precedent in case law and repeated positions taken by the U.S. Congress.

The Copyright Act creates civil and criminal liability for various acts of copyright infringement, but it does not expressly give rise to liability for infringement committed by third parties.[35] Furthermore, the U.S. Supreme Court has defined specific circumstances under which service providers may be held civilly liable (i.e., not criminally responsible) for direct copyright infringement by third parties, such as distributing "a device with the object of promoting its use to infringe copyright."[36]

The fundamental legal problem with this aspect of the government's case is that only Congress can create new criminal liability; judges cannot. Previous instances in which courts have imposed civil liability for secondary copyright infringement – based on application of common law principles – do not apply in criminal proceedings, as federal crimes are "solely creatures of statute."[37] Whatever authority the courts may have had to recognize a contributory theory of copyright liability in the civil context, the courts simply have no power to impose a basis for criminal liability beyond what is expressly authorized by statute.

There have been other cases in which the U.S. Supreme Court rejected attempts by prosecutors to expand criminal copyright liability. In one such case, Dowling v. United States, a California man was charged criminally for selling bootleg recordings of Elvis Presley concerts through the U.S. Postal Service. After the matter had worked its way through the court system, Supreme Court Justice Harry Blackmun succinctly stated the rule that applies equally here: "The precision with which [Congress] has addressed the problem of copyright infringement for profit, as well as the precision with which it has chosen to apply criminal penalties in this area, demonstrates anew the wisdom of leaving it

[35] See MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005) (the Act *"does not expressly render anyone liable for infringement committed by another"* (quoting ***Sony Corp. v. Universal City Studios, Inc.***, 464 U.S. 417, 434 (1984)); Demetriades v. Kaufmann, 690 F. Supp. 289, 291-92 (S.D.N.Y. 1988) (*"Federal copyright law, unlike patent law, does not expressly create any form of derivative, third-party liability."*).

[36] See Id., at 919, 936-37.

[37] See ***Liparota v. United States***, 471 U.S. 419, 424 (1985) (citing ***United States v. Hudson***, 11 U.S. (7 Cranch) 32 (1812)).

to the legislature to define crime and prescribe penalties." [38]

Legal analysts have been quick to decry those occasions when federal courts have usurped the exclusive power of Congress to define criminal conduct. Harvard-educated attorney Jay V. Prabhu, for example, criticized the Supreme Court's 1997 decision in United States v. O'Hagan,[39] which extended criminal liability for insider trading to a partner in a law firm who traded securities using material, nonpublic information he misappropriated from a client. [40] The defendant had committed "fraud on the source," meaning his fraud was directed against the client from whom he misappropriated the information, as distinguished from classic insider trading, which involves fraud on the purchaser or seller of the securities. This so-called "misappropriation theory" of criminal liability was a creation of the courts, not Congress, used to fill a perceived gap in securities regulations. [41]

In the words of Jay V. Prabhu:

> *With aggrandizing boldness and without guidance from Congress . . . the SEC and [U.S. Department of Justice] have consistently asked federal courts for expanding "interpretations" of Section 10(b) that reach far beyond any boundaries ever contemplated by the legislature. . . . These attempted expansions of Section 10(b) all failed, not because the court disagreed with the policies the Government sought to advance, but because the Court adhered to the constitutional principle that Congress must make those policy judgments in legislation it enacts. Any contrary result would violate the long-standing principle that "[i]t is the legislature, not the Court, which is to define crime, and ordain its punishment."* [42]

Mr. Prabhu concluded his critique with a prescient observation, one that applies equally to the prosecution's theory of criminal secondary copyright infringement in the Megaupload case:

[38] ***Dowling v. United States***, 473 U.S. 207, 228 (1985).

[39] ***U.S. v. O'Hagan***, 521 U.S. 642 (1997).

[40] Rule 10b-5 – promulgated by the SEC pursuant to its authority under Section 10(b) of the Securities Exchange Act of 1934 – makes it unlawful for any person to *"engage in any act, practice or course of business which operates or would operate as a fraud or deceit upon any person, in connection with the purchase or sale of any security."*

[41] See Criminalizing from the Bench: The Expansion of Section 10(b) in ***United States v. O'Hagan*** (http://www.fed-soc.org/publications/detail/criminalizing-from-the-bench-the-expansion-of-section-10b-in-united-states-v-ohagan).

[42] Id., at 2 (emphasis added) (internal citations omitted).

> *As one would expect, the SEC has preferred the "flexibility" offered by "case-by-case" determinations, which enables the Government to prosecute "evolving types of conduct . . . [I]t is not the Executive's constitutional role, with the approval of the Judiciary, to criminalize activities.* [43]

Jay V. Prabhu was squarely (and appropriately) on the side of principled constitutionality when he made those observations, which were published in 1998 while he was employed as an associate with Wilmer, Cutler & Pickering, a Washington law firm that had represented Mr. O'Hagan during the SEC's investigation of his case. [44] Interestingly, Jay V. Prabhu later moved from the private practice of law to become a federal prosecutor in the Eastern District of Virginia – and Chief of the U.S. Department of Justice's Cybercrime Unit – from where he personally signed the Megaupload indictment. Thus, the standard Mr. Prabhu called "'[o]ne of the fundamental tenets of our Constitution" when he denounced the Department of Justice's expansion of criminal liability for securities fraud no longer seems to dictate in the context of alleged secondary copyright infringement, now that his current employer is tasked with championing the interests of the Copyright Lobby.

Moreover, unlike the statute governing the O'Hagan case – which created a broad and pliable definition of criminal activity – Congress has had a number of opportunities to expand criminal liability for secondary copyright infringement, but instead has moved in the opposite direction. For example, in 2004, Congress rejected a bill that would have created secondary liability under the Copyright Act. [45] Subsequently, Congress twice amended the Copyright Act's criminal provisions, and both times it omitted any reference to vicarious or contributory liability. [46]

It would be a radical departure to extend secondary liability into criminal proceedings when Congress has taken affirmative steps to scale back even civil liability of this sort. The history of legislative activity in this area confirms that Congress is attuned to the difficulties new technologies can present, seeking to maintain a balance between protection for intellectual property and protection for innovation. The Megaupload indictment tips the scales toward copyright extremism by trying to criminalize innocent businessmen for the unlawful conduct of third parties.

[43] Id., at 3 (emphasis added) (internal citations omitted).

[44] Id., at 4.

[45] See Inducing Infringement of Copyrights Act of 2004, S. 2560, 108th Cong. (2003).

[46] See Prioritizing Resources And Organization For Intellectual Property Act of 2008, Pub. L. No. 110-403, §201(a), 122 Stat 4256 (2008); Family Entertainment And Copyright Act of 2005, Pub. L. No. 109-9, §103(a), 119 Stat 218 (2005).

Notwithstanding the U.S. government's improper attempt to extend criminal liability to alleged secondary infringement, the government's indictment also falls short because it makes no attempt to allege facts that could constitute "double willfulness," namely that Megaupload willfully aided and abetted a willful primary infringer. The government perhaps omitted such allegations because it was aware that Megaupload and its executives took steps to reduce potential copyright infringement by the company's third-party users.

The prosecution's allegation of a "Mega Conspiracy" is not enough to cure its flawed theory of criminal secondary infringement because conspiracy requires "a specific agreement to commit a specific crime."[47] Any "agreement" amongst the defendants could not possibly have contemplated secondary copyright infringement because, as noted, no such crime exists. Moreover, the indictment does not allege any "agreement" between the defendants and the third-party users, nor does it assert even a single instance of direct criminal infringement by any of the users. Therefore, even if secondary infringement were a viable legal theory for criminal liability, the indictment fails to set out a viable case for conspiracy.

b. Substantial Non-Infringing Uses

The U.S. government cannot even argue that the conduct of Megaupload and its executives gives rise to civil liability for secondary infringement, much less criminal liability.

The U.S. Supreme Court decision in Sony Betamax [48] established that distributors of products or services capable of substantial non-infringing uses are not civilly liable for secondary "civil" infringement. The vast scope and scale of non-infringing uses for Megaupload's cloud storage service are so obvious they should require no further elucidation, although the U.S. government apparently fails to see them at all. Users of almost every possible variety – from young children to major multinational corporations – were instantly given access to massive amounts of digital space and bandwidth without the substantial financial outlay that would otherwise have been required to organize computer servers and Internet architecture in their homes or businesses.

At its peak, the Megaupload network was running at a rate of 1.5 terabits per second, equivalent to about 48,000 file transfers per minute. Most of Megaupload's hundreds of millions of hosted files were

[47] See ***United States v. Burgos***, 94 F.3d 839, 860 (4th Cir. 1996).

[48] ***Sony Corp. of America v. Universal City Studios***, Inc., 464 U.S. 417 (1984).

downloaded less than 10 times, many of them not at all, which – contrary to the picture portrayed by the U.S. government – indicates a very high level of protected and lawful use. The Megaupload service was used not only by top business executives, but also by IP addresses originating at the FBI and other U.S. government agencies, among many others.

Furthermore, many legitimate users of the Megaupload service have since come forward. For example, in a somewhat ironic twist, Michael Weinberg, a staff attorney at the rights watchdog Public Knowledge, remarked:

> *As luck would have it, over the weekend I used my home laptop to pull down the stream of the House Judiciary Committee [Stop Online Piracy Act] markup. I wanted to transfer it here to work so that I could cut it up into a video we were using. I uploaded it, but before I had a chance to download it Megaupload was shut down. I can't speak for everything happening on the site, but Megaupload was providing me a completely legitimate service for a completely legitimate end.* [49]

Indeed, the YouTube case and others have already demonstrated that the non-infringing uses of cloud storage and file sharing in today's world are limited only by the imagination of users: emerging musicians seeking to gain exposure by sharing their work with fans; film students on opposite sides of the world trading edits to a documentary in real time; mobile apps developers exchanging modules with users; graphic arts designers delivering work product to their clients . . . yes, even amateur auto-racing enthusiasts sharing race videos with their friends – the very reason Kim Dotcom developed Megaupload in the first place – are engaged in legitimate, non-infringing use. And the potential non-infringing uses are literally infinite.

In light of these realities, the assertion by U.S. prosecutors that Megaupload contrived its business exclusively to facilitate copyright infringement is completely spurious.

Unfortunately, when the U.S. government seized Megaupload's domains and servers, it placed the financial interests of relatively few copyright holders above the interests of millions of legitimate users who were instantly, indefinitely and without warning denied further access to their personal files. According to one report, at least 15,634 U.S. military personnel lost access to their Megaupload

[49] ***"Megaupload wasn't just for pirates: angry users out of luck for now,"*** Ars Tecnica, Jan. 20, 2012 (http://arstechnica.com/gadgets/2012/01/megaupload-wasnt-just-for-pirates-angry-users-out-of-luck-for-now/).

accounts, along with many photos and personal files of soldiers deployed overseas. [50]

In response to the growing number of complaints from users who lost their files, the non-governmental organization Electronic Frontier Foundation (EFF) is taking action. EFF, with the support of the Megaupload legal team, has filed several motions before the court on behalf of entrepreneur Kyle Goodwin seeking the return of his private property, which he contends was expropriated by the U.S. government. Mr. Goodwin used Megaupload to run a business making children's sports videos for parents, and his case underscores the U.S. government's disregard for the rights of legitimate users:

> *In no area of commercial or personal activity is the government allowed to seize property without taking reasonable measures to avoid unnecessary harm and loss of commercial value. That should be no less true when the property is information. Thus, if the government is going to get into the business of seizing Internet properties used to host a wide range of content — infringing and not — it must implement procedures and standards for protecting the property and due process rights of innocents such as Mr. Goodwin who use those services for legitimate purposes. Since the government seems uninterested in developing those processes and standards itself, this case should serve as a starting point for the judiciary to do so.* [51]

The issue of non-infringing use is both dispositive and vital to understanding why the content industry is so exercised over file-sharing services like Megaupload. After Sony Betamax established that distributors of products with substantial non-infringing uses are not liable in civil court for copyright infringement by their customers, the content industry began a frenzied campaign in Washington – which persists to this day – to undermine that doctrine. If the treatment of Megaupload is any indication – they have no plans to give up.

c. Rewards Program Not a Contributor to Infringement

Another glaring falsehood in the U.S. government's indictment is that Megaupload's "Uploader

[50] ***"Megaupload Search Warrant Requests Ignored Massive Non-Infringing Use,"*** Torrent Freak, Nov. 18, 2012 (http://torrentfreak.com/megaupload-search-warrants-ignored-massive-non-infringing-use-121118/).

[51] Brief of Kyle Goodwin in Support of His Motion for the Return of Property Pursuant to 18 U.S.C. § 1963 and/or Federal Rule of Criminal Procedure 41(g) (https://www.eff.org/document/kyle-goodwin-motion-return-property).

Rewards" program aimed to provide "financial incentives to its premium subscribers to upload copies of popular works" to the site, and thereby encourage or contribute to infringement.

Like most of the government's other arguments, that assertion is not only deceptive and wrong, it defies logic. Megaupload's rewards program was not designed to facilitate piracy; its purpose was to grow the user base of the cloud storage site and attract new paying premium members in a copyright-agnostic manner, which is to say, without assessing content or analyzing whether new members would be less or more likely to upload infringing material. In that sense, Megaupload no more intended its rewards program to encourage infringement than an airline's frequent flyer program is calculated to inspire drug smugglers.

Some of Megaupload's competitors in the cloud storage sector – like RapidShare and YouTube – also recognized the potential business value of a rewards program. Although Megaupload discontinued its program in July 2011 – to some extent in response to complaints by the entertainment industry, and without any measurable effect on site traffic – other cloud storage service providers continued their incentive programs long after Megaupload stopped.

Setting aside the motivation behind Megaupload's incentive program, the company took steps to deter infringing uses of cloud storage. The company restricted incentive rewards to files no larger than 100MB, precisely because movie files are almost never smaller than that. Additionally, only paying premium customers – who were required to provide identifying information – were permitted to participate in the program, alerting them that any abuse would not be anonymous. Thus, far from encouraging copyright infringement, Megaupload's incentive program took measures to discourage it, and the government had only to look at the program's Terms and Conditions to understand that.

The U.S. government could not even argue that Megaupload's rewards program would give rise to civil liability for secondary infringement. Encouraging premium subscribers to use cloud storage with their colleagues clearly has substantial non-infringing purposes, and it matters not whether Megaupload benefitted financially from attracting new paying premium members through its rewards program. Further, as noted, the file size limitations and user identification features incorporated into the program demonstrate a desire to discourage infringement, not encourage it.

d. Safe Harbor and Beyond

As with any cloud-storage service, or – for that matter – online services of any kind, Megaupload was susceptible to misuse by some customers. Any service that enables users to upload and share

digital files across the Internet might be used to infringe underlying copyrights. To address this issue and to prevent misuse of the service, Megaupload instituted several measures to comply with global safe-harbor provisions such as the Digital Millennium Copyright Act (DMCA). [52]

To begin with, Megaupload cooperated with copyright owners by following the "notice and takedown" procedures described in the DMCA, and it designated an agent to receive notices from copyright owners. Accordingly, upon receipt of a signed, written notification from a copyright owner credibly identifying the presence of an allegedly infringing work, Megaupload as a matter of course would act expeditiously to remove or disable access to the infringing URL.

The recent federal court decision in Viacom v. YouTube – which upholds the safe harbor provisions of the DMCA by declaring unequivocally that generalized knowledge of infringement does not deprive a service provider of those protections – further highlights the challenges the U.S. government faces in its case against Megaupload.

Additionally, as Professor Goldman has noted, the very fact that Megaupload and its executives believed they were in compliance with the DMCA's safe harbor provisions (even if, for argument's sake, they were not) negates the element of criminal intent required for criminal liability:

> *Criminal copyright infringement requires willful infringement, a very rigorous scienter level. . . . Megaupload's business choices may not have been ideal, but Megaupload has a number of strong potential defenses for its users' activities, including 512(c), lack of volitional conduct and more. Whether it actually qualified for these is irrelevant; Megaupload's subjective belief in these defenses should destroy the willfulness requirement.* [53]

Megaupload went even beyond compliance with the DMCA's safe-harbor provisions. For example, Megaupload negotiated with numerous major copyright holders or their agents – including the Recording Industry Association of America, Disney, Warner Brothers, NBC, and Microsoft – to allow them access to remove directly, without the oversight or involvement of Megaupload, an active link

[52] Broadly speaking, the DMCA "safe-harbor" provisions are a statutory framework that insulates service providers from liability for copyright infringement resulting from the storage of information on their systems or networks at the direction of users. (See 17 U.S.C. § 512(3)(c).)

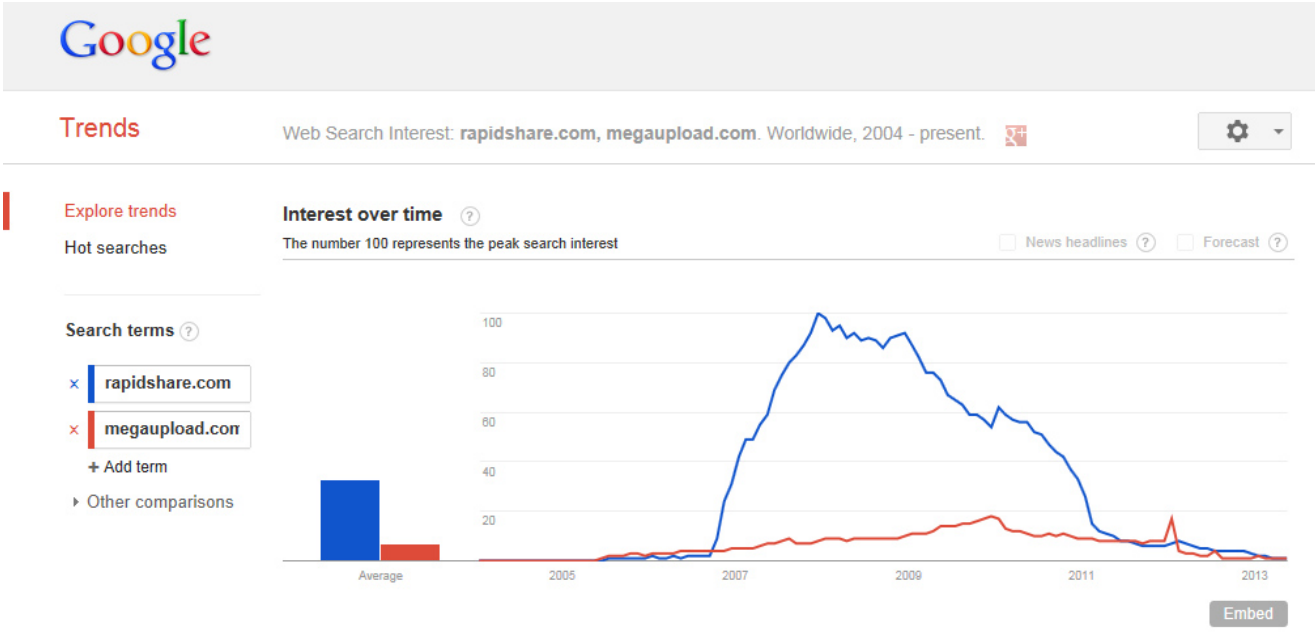
[53] http://blog.ericgoldman.org/archives/2012/04/megaupload.htm.

to material they believed infringed their copyrights. This enhanced access enabled such parties to protect their copyrights without need for formal take-down notices under the DMCA, and resulted in more than 15 million takedowns.

Although not required under the DMCA, the company also implemented various internal measures to discourage infringement. Megaupload required each user to accept its Terms of Use prior to uploading any file to the site. These terms included a prohibition against uploading any digital material or files for which the user did not own the copyright or was not authorized to have and maintain the files.

Megaupload also purposely refrained from creating a searchable index of the files on its servers, and it employed sophisticated mechanisms to prevent search engine crawlers like Google's from doing so. Although the U.S. government has asserted that Megaupload took those measures in order to "conceal the scope of its infringement," the opposite is true. By preventing the development of a searchable index, Megaupload reduced the likelihood that infringing files could be identified and downloaded by other users of the service.

The effectiveness of that anti-piracy measure is illustrated by the following statistic from Google Trends:



As the data demonstrate, Internet search interest in the term "rapidshare.com" – denoted above in blue – consistently exceeded search interest in the term "megaupload.com" by a substantial

margin during the period 2007 through 2011. At the peak of Google's comparison between the two companies, search interest in RapidShare exceeded search interest in Megaupload by a factor of about 20. This can be attributed, at least in part, to the fact that whenever the Google crawler sought to access a Megaupload download link relating to a large file, the company responded with a web page error, signifying that the page was unavailable.

Additionally, Megaupload used caching servers to store content temporarily, a highly protected automated function under the DMCA. [54]

The U.S. government is simply wrong to assert that the DMCA's safe harbor provisions do not apply to Megaupload. The fact is that Megaupload went well beyond its legal requirements to discourage copyright infringement.

e. Colonization of the Internet

The Megaupload case reflects an improper effort by the U.S. government to expand its global reach, prosecuting companies and individuals it believes have violated U.S. law, regardless of where they reside around the world. If U.S. law is properly applied, however, at least two separate legal concepts – personal jurisdiction and extraterritoriality – should operate to curb this trend toward "colonization" of the global Internet.

I. Personal jurisdiction

In addition to all the other legal hurdles the prosecution must face, the U.S. federal court lacks jurisdiction over Megaupload. That impediment comes about because Megaupload is a wholly foreign corporation; it is not incorporated in the United States, and it has no agents or offices in the United States. Consequently, the prosecution has no mechanism to serve criminal process on Megaupload – which in this instance would be a summons – to officially make it party to the criminal proceedings and obligate it to respond in defense of the allegations.

The U.S. Supreme Court has, on multiple occasions, emphasized that service of process is "fundamental to any procedural imposition on a named defendant" and a prerequisite to the

[54] See 17 U.S.C. §512(b).

exercise of the Court's power over it.[55] Consequently, federal courts lack power to assert personal jurisdiction over a defendant "unless the procedural requirements of effective service of process are satisfied."[56]

Ordinarily, criminal defendants are served with process in the form of an arrest warrant. However, because corporate entities like Megaupload are not natural persons and cannot be arrested, they must instead be served with a summons.[57] The procedure for serving such a summons is set out in Rule 4 of the Federal Rules of Criminal Procedure, which says the following:

> *A summons is served on an organization by delivering a copy to an officer, to a managing or general agent, or to another agent appointed or legally authorized to received service of process. A copy must also be mailed to the organization's last known address within the district or to its principal place of business elsewhere in the United States.*[58]

In the case of Megaupload, the company has no officers or agents in the United States to accept service of a summons, nor does it have an office in the United States where a summons could be mailed. Rule 4 requires that both those steps be satisfied, and because neither is possible for Megaupload, the court lacks jurisdiction over the company and the government is foreclosed from prosecuting it.

The prosecution has advanced a handful of arguments why it believes the court is still able to assert jurisdiction over the company. However, none of those theories is even remotely viable.

[55] Murphy Bros., Inc. v. Michetti Pipe Stringing, Inc., 526 U.S. 344, 350 (1999) (***"Service of process, under longstanding tradition in our system of justice, is fundamental to any procedural imposition on a named defendant."***).

[56] ***Omni Capital Int'l, Ltd. V. Rudolf Wolff & Co.***, 484 U.S. 97, 104 (1987).

[57] See, e.g., Sharp v. Commercial Solvents Corp., 232 F. Supp. 323, 326 (ND. Tex. 1964) (noting that "a corporation, . . . cannot be subjected to arrest"); United States v. Schallinger Produce Co., 230 F. 290, 293 (E.D. Wa. 1914) (noting that the "prosecution is against a corporation, where no warrant of arrest is applied for or can be issued").

[58] Fed. R. Crim. P. 4(c)(3)(C) (emphasis added). Rule 9 of the Federal Rules of Criminal Procedure, which applies to warrants and summonses following a grand jury indictment, incorporates Rule 4(c) by reference. See, e.g., Fed. R. Crim. P. 9(c)(1)(A) ("The warrant must be executed or the summons served as provided in Rule 4(c)(1), (2), and (3).").

First, the prosecution has argued that service of process should somehow be suspended simply because Megaupload is aware of the proceedings against it. According to the government, all that should matter is whether the government acted in good faith – itself a dubious starting point for the government in this case – and whether Megaupload was aware of the charges. Of course, that would turn Rule 4 into a mere suggestion. Tellingly, the legal precedents cited by the government in support of this theory all involved cases in which the prosecution mailed a copy of the summons to the relevant U.S. address, as required by Rule 4.

Second, the government has argued that it need not comply with the service requirements of Rule 4 because Megaupload purportedly availed itself of the forum, thereby establishing "minimum contacts" with the United States. However, even if Megaupload has had sufficient contacts with the Eastern District of Virginia to subject it to personal jurisdiction in that forum (which Megaupload does not concede), the U.S. Supreme Court has made clear that proper service of a summons is an additional, separate prerequisite:

> *[B]efore a court may exercise personal jurisdiction over a defendant, there must be more than notice to the defendant and a constitutionally sufficient relationship between the defendant and the forum. There also must be a basis for the defendant's amenability to service of summons.* [59]

Third, the U.S. prosecution assumes it will successfully extradite Kim Dotcom or other officers of Megaupload – at which time the government might be able to serve one of the individuals personally with a summons on behalf of the company and thereby satisfy the first part of Rule 4 – but the prosecution also asserts it may disregard the second part of the rule, which obligates the government to mail a summons to Megaupload. Obviously, there is no guarantee that any of the company's executives will be extradited to the United States, but even if they were, the prosecution is not permitted to discard a required step simply because it cannot fulfill it. Were the government correct, Rule 4's express mailing requirement would become meaningless, and that is not an available interpretation of the law. [60]

Finally, the government argues that, to the extent it must nod at the mailing requirement set out in

[59] ***Omni Capital Int'l, Ltd. V. Rudolf Wolff & Co.***, 484 U.S. 97, 104 (1987).

[60] See ***United States v. Menasche***, 348 U.S. 528, 538-39 (1955) ("It is our duty 'to give effect, if possible, to every clause and word of a statute.'").

Rule 4, it may ignore what the rule actually says and instead mail a summons to an address of its choosing. If the prosecution had its way, it would effectively amend Rule 4 by mailing the summons to: (1) a third-party vendor of Megaupload, Carpathia hosting; (2) some or all of the separately named individual co-defendants; (3) the Commonwealth of Virginia's State Corporations Commission; and/or (4) Megaupload's address in Hong Kong. In addition to ignoring the plain language of Rule 4, this approach also runs contrary to legislative intent. Unlike Rule 4's civil equivalent – which sets out various methods to serve individuals abroad in civil cases, including pursuant to the Hague Convention [61] – Rule 4 contains no comparable provision. The drafters of the legislation clearly intended to exempt wholly foreign corporations from service of criminal process.

The prosecution must have been aware that it could not meet the requirements for service of a summons; indeed, it did not even ask the court to issue one. Nevertheless, the U.S. government saw fit to indict Megaupload, seize all of its assets, and force the company into extinction.

II. Extraterritoriality

The indictment is striking in its geographic scope; it asserts that all Megaupload's global operations and activities – which were predominantly outside the United States – are included in the alleged violations of U.S. copyright law. Setting aside the other reasons why the government's claims lack merit, only infringing conduct occurring within the United States can form the basis of any kind of copyright liability in the United States courts, civil or criminal. Federal statutes such as the Copyright Act do not apply extraterritorially, and the indictment's failure to recognize that limitation presents substantive problems for the prosecution's case, and also has profound implications concerning the propriety of the U.S. government's seizure of all worldwide assets of Megaupload and its executives.

The U.S. Supreme Court recently reaffirmed the principle that federal laws do not apply extraterritorially unless Congress clearly expresses an intent that they should. [62] As for the Copyright Act, Congress has expressed no such intent, and, consequently, numerous federal appellate courts

[61] See Fed. R. Civ. P. 4(f).

[62] ***Morrison v. National Australia Bank***, 130 S. Ct. 2869, 2010 U.S. LEXIS 5257 (2010); see also EEOC v. Arabian American Oil Co., 499 U.S. 244, 248 (1991) (noting that it is a "longstanding principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.'").

have confirmed that it does not apply extraterritorially. [63]

The U.S. indictment of Kim Dotcom overreaches not only with regard to the substantive scope of U.S. criminal laws, but also by attempting to apply them to conduct outside the U.S. The Supreme Court of the United States has made clear that there is a presumption against extraterritorial application of U.S. statutes. [64] "When a statute gives no clear indication of an extraterritorial application, it has none." [65] This reflects the "presumption that United States law governs domestically but does not rule the world." [66]

Yet at least four of the five counts of the U.S. indictment against Kim Dotcom rest on statutes that give no clear indication that they apply outside the U.S.[67] There is thus a presumption that they do not apply outside the U.S. – where Kim Dotcom is a citizen and resides, and where Megaupload has its offices, installations and the vast majority of its Internet servers.

Megaupload's use of a relatively small number of U.S. servers cannot suffice to evade the presumption against extraterritorial application of the RICO and other statutes used against the company and Kim Dotcom. As one U.S. court has observed, "[S]imply alleging that some domestic conduct occurred cannot support a claim of domestic application. '[I]t is a rare case of prohibited extraterritorial application that lacks all contact with the territory of the United States.' ... [S]lim contacts with the United States ... are insufficient to support extraterritorial application of the RICO statute." [68]

[63] See ***Nintendo of America, Inc. v. Aeropower Co.***, 34 F.3d 246, 249 n.5 (4th Cir. 1994) (noting because the Copyright Act has no "expansive statement of its intended reach, it is "generally considered to have no extraterritorial application"); Subafilms, Ltd. V. MGM-Pathe Communications Co., 24 F.3d 1088, 1095 (9th Cir. 1994) (en banc) (describing the "undisputed axiom" that U.S. copyright law has no extraterritorial application); Palmer v. Braun, 376 F.3d 1254, 1258 (11th Cir. 2004) ("[I]t is only where an infringing act occurs in the United States that the infringement is actionable under the federal Copyright Act . . ."); Robert Stigwood Group Ltd. V. O'Reilly, 530 F.2d 1096, 1101 (2d Cir. 1976) ("Copyright laws do not have extraterritorial application.")

[64] E.g., ***Kiobel v Royal Dutch Petroleum Co.***, 2013 U.S. LEXIS 3150, at 10 (2013); Morrison v. National Australia Bank Ltd, 130 S. Ct. 2869, 2878 (2012).

[65] ***Kiobel***, 3150, at 10, quoting Morrison, at 2878.

[66] ***Kiobel***, 3150, at 10, quoting Microsoft Corp. v. AT&T Corp., 550 U.S. 437, 454 (2007).

[67] Count 1: 18 U.S.C., 1962(d) (RICO); Count 2: 18 U.S.C. 371 (conspiracy); Counts 4 and 5: 18 U.S.C. 2, 18 U.S.C. 2319 and 17 U.S.C. 506 (copyright infringement). Only Count 2: 18 U.S.C. 1956 (h) (money laundering) rests on a statute that expressly refers to certain conduct outside the US, but it is not clear that Kim Dotcom or Megaupload engaged in any such conduct.

[68] ***Norex Petroleum Ltd. v. Access Industries Inc.***, 633 F. 3d 29 (2d Cir. 2010) (civil RICO case).

For the same reason, it is doubtful that U.S. courts even have jurisdiction over the case against Kim Dotcom and Megaupload. As the U.S. Supreme Court has admonished, "attenuated connections" to the U.S. "fall far short of the 'the continuous and systematic general business contacts' necessary for general jurisdiction." [69] The Court properly cautioned against the "sprawling view of general jurisdiction" by which "any substantial manufacturer or seller of goods would be amenable to suit, on any claim for relief, wherever its products are distributed." [70]

Only about 10% of Megaupload users were resident in the United States; the remaining 90% were located abroad. Further, the indictment itself acknowledges that the vast majority of Megaupload's activities occurred outside the United States. Among other things, the indictment confirms that: (1) Megaupload was organized outside the United States and had no offices in the United States; (2) the individual defendants are all foreign citizens who reside abroad; and (3) a substantial portion of Megaupload's storage capacity was located in such places as The Netherlands, Canada, France and "around the world."

With respect to the conduct of Megaupload's users, the indictment consistently omits any mention of the location of the conduct it describes, and it specifically does not allege that any of the purported copyright infringement upon which it bases its theory of criminal secondary infringement occurred inside the United States. To the extent the indictment alleges anything about the location of purportedly unlawful conduct, it seems to suggest that it occurred abroad. [71]

Although the indictment does allege that Megaupload controlled some servers located in Virginia, the existence of domestic servers with material uploaded by third parties is insufficient to trigger application of substantive U.S. copyright law. There must be at least some conduct that causes, in a meaningful way, an infringement. [72] If this were not so, the U.S. Supreme Court could not have held – as it did in Sony – that a manufacturer of copy machines, possessing constructive knowledge that purchasers of its machines may be using them to engage in copyright infringement, was not

[69] ***Goodyear v. Brown***, 131 S. Ct. 2846, 2856 (2011).

[70] Id.

[71] Some examples in the indictment include: (1) ¶73(v), describing user's files as "Vietnamese content" and "Italian series" [sic]; (2) ¶73(tttt), referring to complaint by Taiwanese broadband service provider whose customers were having trouble downloading material; (3) ¶73(nnn), referring to infringement reports from Mexico; (4) ¶73(ppppp), referring to complaint from Vietnamese Entertainment Content Protection Association regarding allegedly infringing links.

[72] CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 549-50 (4th Cir. 2004) (direct infringement requires more than "mere ownership of a machine used by others to make illegal copies . . . [there] must be actual infringing conduct.").

strictly liable for infringement. [73] In the case of Megaupload, file transfers by the users of the service did not require any conduct by the defendants, either inside or outside the United States, because the systems were neutral and entirely automated.

Thus, the prosecution's legal case faces significant challenges on extraterritoriality grounds. Even if there were such a thing as criminal liability for secondary copyright infringement – and even if the defendants resided in the United States at the time of the alleged offense – they could not be held secondarily liable for direct infringement committed outside the United States. [74] Moreover, the indictment's allegations of conspiracy do not overcome these hurdles, for the same reasons they do not resolve the government's theory of criminal secondary infringement. The indictment does not allege any agreement between the defendants and the Megaupload users to commit a specific crime, and any agreement between the defendants themselves could not have related to criminal conduct.

Equally as important, any proceeds traceable to wholly foreign conduct lacking a U.S. nexus could not be seized pursuant to federal forfeiture provisions. [75] Consequently, given the indictment's failure to allege the location of purportedly infringing activity – together with the implication from some of its allegations that most of the activity occurred outside the United States – an argument could be made that there was no legitimate intent to the U.S. government's worldwide seizure order, even if the prosecution's theories about criminal liability were not flawed.

The U.S. government applied for its seizure order on an ex parte basis – behind closed doors, without notifying Megaupload – the prosecution alone making its case to a magistrate judge. Nobody was present to represent the interests of Megaupload and its executives, and nobody explained the various reasons a seizure order against all worldwide assets of the defendants would be inappropriate. Further, because a summons has not been served on Megaupload, the company remains unable to challenge the scope or any other aspect of the seizure, and the government will

[73] Id., at 549; see also ***ALS Scan, Inc. v. RemarQ Communities, Inc.***, 239 F.3d 619, 622 (4th Cir. 2001) ("As to direct infringement, liability is ruled out for passive, automatic acts engaged in through a technological process initiated by another." (quoting H.R. Rep. No. 105-551(1), at 11 (1998)); Cartoon Network LP, LLP v. CSC Holdings, Inc., 536 F.3d 121, 131-32 (2nd Cir. 2008) (direct infringement requires "volitional conduct," not mere ownership of device used by others to infringe).

[74] See ***Subafilms, Ltd. V. MGM-Pathe Communications Co.***, 24 F.3d 108, 1093 (9th Cir. 1994) (en banc) ("[A] primary activity outside the boundaries of the United States, not constituting an infringement cognizable under the Copyright Act, cannot serve as the basis for holding liable under the Copyright Act one who is merely related to that activity within the United States." (quoting 3 Nimmer, § 112.04[A][3][b], at 12-86)).

[75] See 18 U.S.C. § 981(a)(1)(C) (identifying as property subject to forfeiture such property constituting or derived from proceeds traceable to a violation of enumerated statutes, including the Copyright Act) (emphasis added).

not agree to release even a penny to pay for the company's legal defense or to preserve the evidence on Megaupload's servers. It is hard to imagine a more unfair outcome.

Limits on extraterritorial application of U.S. law – like the requirements or serving corporate entities with a summons – serve a vital role in guarding against prosecutorial overreach and protecting international sovereignty by limiting the U.S. government's ability to reach around the globe and selectively prosecute in the U.S. courts any foreign corporation it deems to have violated U.S. law, even if the conduct is entirely legal where the corporation is located. The Megaupload prosecution demonstrates astounding hubris by the U.S. government, which has now moved to "colonize" the global Internet under its legal jurisdiction, without the slightest bit of respect for the sovereignty of other countries or their views about the boundaries of criminal liability for copyright infringement.

Representatives of other countries have noticed this trend and voiced their concerns. Sixteen Members of the European Parliament, for example, expressed their views to Victoria Espinel, United States Intellectual Property Enforcement Coordinator for the White House:

> *In recent years we have observed the growing reach of US laws beyond its territory, also with regards to [intellectual property rights (IPRs)]. The effect is most notable on the internet, where the US Congress proposed laws which would have detrimental and adverse effects on Europe's internet freedom. We are concerned about developments in this direction.*
>
> *When the US Department of Justice effectively closed down the file hosting service MegaUpload, it seized servers and domain names with the cooperation of local law enforcement agencies in Hong Kong and New Zealand, but also in EU Member States. The credibility of effective extraterritorial IPR enforcement concerns us. Equally alarming is the envisaged extradition of a British EU citizen due to copyright infringements, or the blocking of Spanish websites, which likely did not infringe Spanish law. Given the importance of a solid transatlantic relation, we urge you to consider the negative extraterritorial impact of US law.*
>
> *We fully appreciate that acts in Europe or third countries may be considered criminal in the US and may have an effect on stakeholders within your territory. However, we would like to stress that the rigorous extraterritorial enforcement of US IP law on the internet is not a sustainable way to address the challenges stemming from the internet in relation to IPR protected media.*[76]

[76] http://infojustice.org/wp-content/uploads/2012/08/Members-of-the-European-Parliament.pdf.

f. Due Process Violations

I. Mischaracterization of facts and omission of exculpatory evidence

One of the most damaging abuses by the U.S. prosecution team was its mischaracterization of facts and omission of exculpatory evidence from its applications for search warrants whereby it seized Megaupload's domain names. Megaupload was in the process of cooperating with a U.S. government investigation into alleged infringement by a third-party user of the service. Megaupload purposefully left intact certain infringing movies identified to it by the government, in order to preserve the status quo and the integrity of the FBI's investigation. Subsequently, in its applications for search warrants to seize the company's domain names, the government would tell the federal court that the company had been told about those infringing movies, but had failed to take them down, omitting the fact that Megaupload did so in order to cooperate with the ongoing investigation. The prosecution's selective omission flipped the import of the facts on their head, turning willful cooperation into criminal intent. Moreover, the government's twisted characterization was the only direct evidence of intent it offered to the court in support of its applications. Had the exculpatory evidence been included in the applications, it seems likely that the warrants could not have issued.

From Megaupload's viewpoint, it is difficult to imagine a more abusive tactic. These warrants were requested from a federal magistrate judge on an ex parte basis; Megaupload was not present in court to correct the prosecution's story or to explain why the warrants should not issue. In those circumstances, it is incumbent upon the U.S. government to act properly, to be forthright, not to omit key facts selectively to suit its purpose. Megaupload has since challenged the validity of the warrants, but it is too late; the company became extinct the moment its domain names were seized. In the face of all this, although the defendants are the ones that have been branded "pirates," prosecutorial piracy seems a more apt characterization of the facts.

II. Illegal activity in New Zealand

To assist in the investigation and prosecution of Megaupload and Kim Dotcom, the U.S. government recruited the New Zealand authorities, which in the process engaged in various illegal activities in New Zealand. Although some of the facts are still being uncovered, it is undisputed that the New Zealand authorities illegally spied on Kim Dotcom prior to his arrest, and continued to spy on him illegally for an additional ten days after the arrest. They also carried out the raid on his home in Coatesville on the basis of illegal search warrants. While the ultimate repercussions of those illegal activities are still unclear, it is safe to say that they lend no credibility to the U.S. prosecution's case against Megaupload and Kim Dotcom.

4 The Story Behind the Story: A Contract Prosecution

The U.S. government's attack on Megaupload and Kim Dotcom is driven largely by the influence the MPAA has wielded historically in Washington on behalf of its member copyright holders, and more particularly by the vigor with which it has exercised its financial resources to instrumentalize the current White House and other branches of government. While the U.S. government falsely (albeit dramatically) accuses Megaupload of engaging in a "Mega Conspiracy," the real conspiracy – the actual, concerted agreement between two people to carry out a wrongful plan – may lie between old colleagues, both longstanding members of the world's most exclusive club, former Senator Chris Dodd (D-Connecticut) and former Senator Joe Biden (D-Delaware). Together they conceived and executed the attack on Megaupload, and it can be argued that both men benefitted from it. On the one hand, Joe Biden delivered to Chris Dodd the takedown of a major perceived threat to the MPAA's copyright holders; on the other hand, Chris Dodd delivered to Joe Biden the continuing political and financial support of Hollywood during the White House's critical 2012 reelection campaign.

To assert that Chris Dodd and Joe Biden have a history together would be to say that ham is acquainted with eggs. Chris Dodd served in the U.S. Senate for almost 30 years – from 1981 through 2010 – while on his part, Joe Biden ranks as the 16th longest serving senator in U.S. history (36 years and 13 days), holding that office from 1973 through his elevation to the vice-presidency in January 2009. [77] On the occasion of Chris Dodd's retirement from the Senate to jump directly into the role of Chairman and CEO of the MPAA, Vice President Biden had this to say:

> *Senator Dodd is one of my best friends in life. We served together in the Senate for almost 30 years, and to every meeting, every hearing, every floor debate, he brought a keen intellect and a deep understanding of the subject matter on every issue. . . . I count myself lucky because I know he's not going too far and will always be [a] source of advice and counsel. . . .* [78]

It is no secret that the MPAA has long considered Megaupload a threat to its current business model. Media reporting confirms that the MPAA had already compiled extensive information about

[77] http://www.senate.gov/senators/Biographical/longest_serving.htm.

[78] http://www.cbsnews.com/8301-503544_162-12005-503544.html.

Megaupload's "operations and management" when it complained about the company to U.S. federal authorities, sparking an FBI probe beginning in March 2010. [79] And although Megaupload is hardly the only internet-based operation the MPAA considers guilty of sustaining global piracy and counterfeiting, its animosity toward Megaupload seems strangely personal. In the MPAA's November 2010 submission for the U.S. Trade Representative's Special 301 Notorious Markets Review – an annual list compiled by the USTR based on comments from industry purporting to identify foreign markets "where counterfeit and pirated products are prevalent" – the MPAA revealed some of its hostility. While treating every other enterprise on its list dispassionately, the MPAA gratuitously jabbed Megaupload with this:

> *Torrent Freak did a story on Megaupload, "The Mega-Money World of MegaUpload" which describes MegaUpload as "one of the most prominent file-hosting services on the Internet. It is owned by an unbelievably colorful individual who is probably better known for his multiple convictions for computer fraud, embezzlement and insider trading."*

After Chris Dodd took over as Chairman and CEO of the MPAA in March 2011, the MPAA – already known for aggressive lobbying – turned up the pressure in Washington to deal with the perceived threat presented by Megaupload and other web-based technologies. During the first quarter of 2011, roughly coinciding with Chris Dodd's arrival at the helm, the MPAA boosted its lobbying disbursements by 17% over the previous quarter. Not surprisingly, Joe Biden was the MPAA's most prominent political contact during this period, apparently fulfilling the Vice President's own prediction a few weeks earlier that Chris Dodd would continue to provide "advice and counsel" after leaving the Senate. While passage of SOPA and PIPA were undoubtedly on the MPAA's lobbying agenda, it is also clear that "rogue sites" were part of the discussion. [80]

Chris Dodd's willingness to lobby on behalf of the MPAA was never more evident than during the lead-up to Congressional action on SOPA:

[79] http://news.cnet.com/8301-31001_3-57369825-261/nobody-wanted-megaupload-busted-more-than-mpaa/.

[80] http://www.digital-digest.com/news-63052-MPAA-Reveals-400000-Spend-on-Q1-Lobbying-of-Law-Enforcement-Agencies.html.

> *Candidly, those who count on quote "Hollywood" for support need to understand that this industry is watching very carefully who's going to stand up for them when their job is at stake . . .. Don't ask me to write a check for you when you think your job is at risk and then don't pay any attention to me when my job is at stake.* [81]

Ultimately, the legislation failed to pass because there was overwhelming public outcry against it, not because the Administration did not support the measure. The day after Chris Dodd made his threat, the U.S. government struck, Megaupload was shut down, its worldwide assets were seized, and its executives were thrown in jail. Not only did the MPAA and the U.S. government machinate behind the scenes to take down Megaupload and Kim Dotcom, they have worked hand in glove to prejudice the defense by tainting the public's perception of the company and its founder. The objective has been to employ the dramatic raid, the voluminous indictment and ready media access to paint an undesirable image of Kim Dotcom, the dangerous criminal mastermind, living large with his ruthless gang of cohorts off the spoils of a pernicious global buccaneering enterprise.

The public smear began even before the take-down, with the U.S. government tipping the media in advance, then quickly providing copies of the massive 72-page indictment for public distribution. The indictment itself invokes RICO, a statute enacted to combat organized crime. The claims hinge almost entirely on allegations of conspiracy, using that term no less than 304 times, inventing the expression "Mega Conspiracy" as if there were some clever humor in it. It advances the absurd idea (among others) that Megaupload – a leader in world-wide cloud storage services – was created and operated solely for the purpose of facilitating copyright infringement, casting Kim Dotcom and his fellow executives as nothing more than marauders.

But the language in the indictment was only the beginning. Nobody can seriously challenge the notion that the early morning raid on Kim Dotcom's home was needlessly theatrical. The dozens of armed agents decked in body armor, the attack dogs, the helicopter deployment – the entire production was crafted for the camera. It was an overdone charade, an elaborate version of the "perp walk" designed to prejudge the accused, to lay on a guilty verdict through imagery rather than the justice system. Civil libertarian Nat Hentoff rightly commented that, subject to such treatment, "Mother Teresa would look extremely suspicious, especially if her hands were cuffed behind her back." [82]

[81] See http://www.foxnews.com/politics/2012/01/19/exclusive-hollywood-lobbyist-threatens-to-cut-off-obama-2012-money-over-anti/.

[82] http://www.economist.com/node/18929399.

The MPAA's rhetoric has only sharpened since. Shortly after the takedown, Chris Dodd began to speak publicly about Megaupload and Kim Dotcom as examples of "the piracy problem." In an address to the National Association of Attorneys General on March 5, 2012, he said:

> *Infringing copies of movies were viewed uncounted millions of other times by accessing links on cyberlockers such as Megaupload, by streaming from largely foreign websites and through other technological means.*
>
> *In the Megaupload case, federal investigators tell us that the man known as Kim Dotcom and his colleagues made more than $175 million through subscription fees and online ads while robbing authors and publishers, movie makers, musicians, video game developers and other copyright holders of more than $500 million.*
>
> *Some continue to argue that the debate about piracy and counterfeiting is not about the money. Don't believe it. As a famous 20th century pundit H.L Mencken was fond of saying, "When they tell you it's not about the money...it's about the money." Just look at Mr. Dotcom. . . .* [83]

Examples of similarly disparaging publications by the MPAA's agents are abundant. On February 26, 2012, the MPAA's Senior Vice President for Content Protection, Kevin Suh, called Kim Dotcom "the biggest copyright infringer in the world." [84] During an interview with the Spanish newspaper ABC on January 27, 2013, Chris Dodd referred to Kim Dotcom as "a serial criminal." [85] When Kim Dotcom unveiled a new file sharing service in January 2013, the MPAA published a statement saying that "Kim Dotcom has built his career and his fortune on stealing creative works." [86]

All of these public comments fit the broader themes of the U.S. government's indictment and prosecution. By combining allegations of a massive global conspiracy with the image of pirates set on nothing other than plunder, the U.S. government and the MPAA together have cut sharply in the direction of depriving the defendants of their presumption of innocence.

[83] http://www.mpaa.org/Resources/413d47b5-fa52-4009-aa14-c634b50638e1.pdf, at 4.

[84] See http://www.huffingtonpost.com/2012/02/26/kim-dotcom-megaupload-fou_n_1302343.html.

[85] See http://www.abc.es/cultura/20130125/abci-pirateria-rajoy-hollywood-christopher-201301241744.html.

[86] See http://www.thewrap.com/movies/column-post/mpaa-sounds-piracy-alert-kim-dotcoms-new-file-sharing-site-73831.

5 The Copyright Lobby, State Capture and the Human Rights Problem

Unlike physical property rights, protecting intellectual property rights is not a straightforward proposition, but requires a balance between incentivizing creativity by penalizing infringement, and ensuring public access to information and knowledge. In the United States, this balance is left to Congress:

> *The process by which the terms and scope of copyright are decided is a political one. This means that as it designs the contours of copyright, Congress will be picking winners and losers.*
>
> ***
>
> *Copyright's political problem is a classic case of concentrated benefits and diffused costs. Hollywood, the music industry and book publishers reap the rewards of increased protection, while the public bears the costs. The copyright industries can easily organize themselves into lobbies that have every incentive to invest heavily in acquiring greater protections, while individual members of the public, the nominal beneficiaries of copyright, face a collective action problem that keeps them from organizing against stronger copyright laws.* [87]

The natural political dynamic in favor of legislation that protects copyright holders is reflected in the evolution of copyright law over the years. The original Copyright Act of 1790 contemplated a 14-year term of protection for authors of creative works, renewable by request for a second 14-year term. These rights were expanded in 1831 and 1909, along with criminal statutes for infringement, but the system remained voluntary; authors were required to request protection and to file for renewal.[88]

When the U.S. Congress passed the Copyright Act of 1976, it expanded copyright protections dramatically, covering the entire life of the author plus an additional 50 years, and all works were

[87] Brito, Jerry. "Why Conservatives and Libertarians Should be Skeptical of Congress's Copyright Regime." Copyright Unbalanced: From Incentive to Excess (Mercatus Center at George Mason University (November 29, 2012).

[88] Tom W. Bell. "Five Reforms for Copyright" Copyright's Future (2012).

automatically covered and renewed without any registration requirements. [89] In 1999, Congress enacted the Sonny Bono Copyright Term Extension Act – which coincided with the upcoming expiration of a Disney Corporation copyright – and extended the term of coverage retroactively by an additional 20 years. [90]

Felony criminal liability for copyright infringement was not enacted until 1982, and it probably would have never come about but for the lobbying efforts of the MPAA:

> *The MPAA and the [Recording Industry Association of America] were not successful in their lobbying attempts until 1982, when Congress enacted Title 18, Section 2319 of the United States Code. Section 2319 provided for felony penalties for the conviction of reproducing or distributing a certain specified number of records, motion pictures, or audio visual works within a 180 day time period. This was the first time that Congress considered it necessary to provide for felony sanctions, although it limited circumstances, for criminal copyright infringement.* [91]

Criminal and civil copyright statutes were strengthened repeatedly in the years that followed. All told, the Copyright Lobby has successfully expanded copyright protections and stiffened penalties for infringement no fewer than 15 times between 1978 and 2008. [92]

As noted, however, the U.S. Congress has not fulfilled the Copyright Lobby's desire to expand criminal liability to cover secondary copyright infringement. Nevertheless, that obstacle did not deter the MPAA insofar as Megaupload and Kim Dotcom were concerned; the MPAA simply used its influence in Washington – including the Dodd/Biden relationship – to persuade the U.S. Department of Justice to push the legal envelope and charge the crime the MPAA wished existed. The fact that the MPAA was able to accomplish such a feat leads to the conclusion that the MPAA presently enjoys a form of State Capture over the executive branch of the U.S. government.

[89] ***"Copyright Duration and the Mickey Mouse Curve,"*** by Tom W. Bell (http://techliberation.com/2009/08/06/copyright-duration-and-the-mickey-mouse-curve/).

[90] Id.

[91] ***Intellectual Property and Computer Crimes*** by Peter Toren, Law Journal Seminars Press; Lslf edition (July 26, 2003).

[92] ***"How Much Is Enough? We've Passed 15 'Anti-Piracy' Laws In The Last 30 Years,"*** Tech Dirt, Feb. 15, 2012 (http://www.techdirt.com/articles/20120215/04241517766/how-much-is-enough-weve-passed-15-anti-piracy-laws-last-30-years.shtml).

The concept of State Capture was used originally by World Bank academics to describe parts of the former Soviet Union marked by illicit, non-transparent private payments to officials in order to influence the formation of laws, rules, regulations or decrees by state institutions. In the capture economy, "the policy and legal environment is shaped to the captor firm's huge advantage, at the expense of the rest of the enterprise sector." [93]

It is doubtful, of course, that the MPAA or others in the Copyright Lobby are involved in direct payments to corrupt U.S. government officials. The Copyright Lobby has gradually increased its influence by diffusing it around (among other things) direct lobbying, political action committees, campaign donations, and grants to a variety of charitable organizations that in effect advance its political interests. These efforts have led to favorable treatment from the U.S. government in a number of areas, including access to: (1) favorable tax deductions at both the state and federal levels; (2) the domestic legislative drafting process; (3) the U.S. diplomatic apparatus to advance its legislative agenda overseas; (4) the U.S. Trade Representative, which prepares annual Special 301 reports which blacklist "notorious foreign markets" where infringement is prevalent; and (5) the negotiation process for foreign trade agreements, which permits the MPAA to insert favorable terms into such treaties.

Some might argue that the Copyright Lobby and the MPAA are simply doing what every other industry sector in the United States does, albeit perhaps more effectively. And while that may be true, even if the historically favorable treatment of the Copyright Lobby does not rise to the level of State Capture, the calculus clearly shifted under Obama Administration, which – according to "a long-time Obama advisor" – has a practice of turning a blind eye to the revolving door between the White House staff and the content industry:

> *Within Obamaworld, there are a few unwritten rules about how to parlay one's experience into a handsome payday. There is, for example, a loose taboo against joining a K Street lobbying shop and explicitly trading on administration connections. And while joining a consulting firm is acceptable, those who do are reluctant to work for clients reviled by liberals: gun makers, tobacco companies, Big Oil, union busters. Above all, there is a simple prohibition against excessive tackiness. "It's like: Don't embarrass yourself. You were part of something special," says a longtime Obama adviser. "I think if [Obama] were to send an all-staff e-mail, it would be along the lines of Ron Burgundy—'Stay classy, San Diego.' "*

[93] ***"Seize the State, Seize the Day: State Capture, Corruption and Influence in Transition,"*** by Joel S. Hellman, Geriant Jones, and Daniel Kaufman, World Bank Policy Research Working Paper No. 2444 (September 2000) (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=240555).

***

> *There's also the entertainment industry, which is "a for-profit corporate space that's a safe area for Democrats," says a former White House staffer. "You can go work for Harvey Weinstein and make all this money." Obama aide Michael Strautmanis recently left to help oversee "corporate citizenship" at Disney, and Jim Gilio, a White House spokesman, now represents talent at a Los Angeles entertainment law firm.* [94]

Chris Dodd's jump from the U.S. Senate into the cockpit of the MPAA was an equivalent move. As the new Chairman and CEO of the MPAA, Chris Dodd improperly leveraged his friendship with Joe Biden to achieve the MPAA's objectives. Former Senator Dodd's relationship with the Vice President– who comes off manipulated, a cheerfully credulous facilitator – together with the Obama Administration's ravenous hunger for campaign contributions, has given the MPAA absolute control over how the U.S. Department of Justice plays the game in enforcing copyright law. This capture is nowhere more clearly demonstrated than in the Megaupload/Kim Dotcom prosecution.

Professor Goldman has some ominous predictions about where this road leads:

> *The government has also been shockingly cavalier about the collateral consequences of its prosecution on the marketplace. Legitimate web hosts, and their investors, are quaking in their boots that they will be next. It doesn't help that the content industry is circulating a "kill chart" of its next desired targets.*
> *In the end, the Megaupload prosecution demonstrates that SOPA advocates are inevitably going to win. The content owners' ire toward "foreign rogue websites," combined with the administration's willingness to break the law, if necessary, to keep content owners happy, leads to lawless outcomes like the Megaupload prosecution and ICE's domain name seizures.* [95]

These State Capture characteristics, and the Megaupload case in particular, also raise serious human rights issues. In addition to violating the Article 19 Principles on Freedom of Expression and

[94] http://www.newrepublic.com/article/112906/where-obama-staff-veterans-are-working-2013.

[95] http://blog.ericgoldman.org/archives/2012/04/megaupload.htm.

Copyright in the Digital Age, the seizure of the property of Kim Dotcom and of all property worldwide of Megaupload, and of the property of users of their file storage service, together with the effective destruction of Megaupload as a business – all in an ex parte hearing without prior notice, hearing, or opportunity for defense, and with no effective remedy afterward – flagrantly violates internationally guaranteed human rights to property, due process of law, and personal honor. Even if Kim Dotcom had been a suspected terrorist – let alone an Internet entrepreneur – this sort of "shoot first, trial second" justice would offend minimum requirements of the Rule of Law.

The rights to due process of law, property and other internationally guaranteed human rights have repeatedly been vindicated – in cases involving seizures of the property of alleged terrorists – by international tribunals. These tribunals have consistently vindicated the rights of individuals who were publicly listed by the United Nations Security Council as suspected terrorists, and whose assets were then frozen, without being afforded prior notice or opportunity for hearing.

One such case was decided by the UN Human Rights Committee. The Committee hears complaints of violations of the International Covenant on Civil and Political Rights -- to which both the United States and New Zealand are parties. In that case Belgium had sent the names of the complainants to the UN Security Council as suspected terrorists, "even before the [victims] could be heard." [96] The Committee noted their complaint that "they were placed on the sanctions list and their assets frozen without their being given access to 'relevant information' justifying the listing, ..." [97]

The Committee found a resulting violation of their right to travel. [98] It also found a violation of their right to "honour and reputation, in view of the negative association that some persons could make between the authors' names and the title of the sanctions list. Moreover, many press articles that cast doubt on the authors' reputation have been published, ..." [99]

Kim Dotcom is a victim of violations of the same rights: as a result of the ex parte US procedures, he effectively cannot travel, and serious damage has been inflicted on his reputation. Because the Belgian victims had access to judicial remedies before Belgian courts, the UN Human Rights Committee found no violation of their right to an effective remedy. In contrast, Kim Dotcom is not a

[96] ***Sayadi and Vink v. Belgium***, Comm. No. 1472/2006, Views of the Human Rights Committee, UN Doc. CCPR/C/94/D/1472/2006, 29 December 2008, at ¶ 10.7.

[97] Id., at ¶ 10.8.

[98] Id., at ¶ 10.8.

[99] Id., at ¶ 10.13.

U.S. citizen and does not reside in the US. He has no effective U.S. judicial remedy – unless he were to submit to the jurisdiction of the very courts against which he complains.

International and national courts have found similar violations of the rights of other persons publicly listed on the UN Security Council terrorist sanctions list without prior notice or hearing. In the case of one such victim, the Grand Chamber of the European Court of Human Rights ruled that Switzerland violated his rights to freedom of movement and to an effective remedy. [100]

The European Court of Justice found that the European Council of the European Union violated the right to an effective remedy of another victim thus placed on the UN Security Council sanctions list. [101] Notably, the Court also found a violation of his right to property. The Court reasoned that "the contested regulation, in so far as it concerns [the victim], was adopted without furnishing any guarantee enabling him to put his case to the competent authorities, in a situation in which the restriction of his property right must be regarded as significant, having regard to the general application and actual continuation of the freezing measures affecting him." The freezing of his funds therefore "constitute[d] an unjustified restriction of [his] right to property." [102]

Finally, the British Supreme Court found that the British Government exceeded its powers in freezing a victim's assets, after he had been placed on the UN Security Council sanctions list without prior notice or hearing. [103] The precise contours of the violations of due process of law and of the rights to an effective remedy, freedom of movement, honor and reputation, and property, of course differ in these cases from the specific form of the violations in the case of Kim Dotcom. But if anything, the supposed justifications for the use of unfair procedures against suspected terrorists were far stronger than in a copyright case like the one brought against Kim Dotcom and Megaupload.

The bottom line, as recognized by the European Court of Justice, in all cases – in copyright cases no less than in terrorism cases – is that "fundamental rights" must be respected "in a community based on the rule of law ..." [104] If the prosecution of Kim Dotcom is allowed to proceed, not only he, but the fabric of the rule of law, will be at risk.

[100] ***Nada v. Switzerland***, Application No. 10593/88, Judgment of 12 September 2012.

[101] Judgment of the ECJ in Joined Cases C-402/05 P and C-415/05 P, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the EU and Commission of the EC (ECJ Judgment), Sept. 3, 2008, par. 349, available at http://curia.europa.eu/en/content/juris/index.htm.

[102] Id., at ¶¶ 368-70.

[103] ***Ahmed and others v. HM Treasury***, Judgment of 27 January 2010 [2010] UKSC 2.

[104] Kadi, supra, at ¶ 316.

6 Conclusion

The U.S. government's take-down of Megaupload and Kim Dotcom has ramifications far beyond a single company and its executives. It sets an alarming precedent for regulation of the Internet, freedom of expression, privacy rights, and the very Rule of Law. The U.S. government should not be able to act outside the bounds of due process, at the behest of special interest lobbies, to destroy foreign-owned business enterprises and expropriate the private property of millions of individuals.

In response to the unlawful conduct of the U.S. government, the U.S. House Committee on Oversight and Government Reform and the Office of Professional Responsibility of the U.S. Department of Justice should conduct an investigation and hearings into the conduct of the Megaupload prosecution by the U.S. Department of Justice. In particular, the issue of special-interest influence over the executive branch and the failure of the Department of Justice to protect Megaupload consumer data access should be scrutinized.