**MegaBust’s MegaQuestions Cloud the Net’s Future**

**By Philip S. Corwin**

Mid-January 2012 marked a major inflection point for digital copyright policy in the United States:

* On Saturday, January 14th the White House issued a policy statement in response to an online petition against pending anti-piracy legislation signed by more than 100,000 individuals. While supporting efforts to curb infringement of U.S. intellectual property by foreign websites, it outlined that to be acceptable to the Obama Administration any such legislation must guard against online censorship, be narrowly targeted at websites currently beyond the reach of U.S. law, have strong due process protections, be targeted at criminal activity, and not inhibit innovation. The statement was interpreted as indicating that current versions of the Protect IP Act (PIPA) and the Stop Online Piracy Act (SOPA) were not acceptable to the President – although no explicit veto threat was made.
* On Tuesday, January 18, an unprecedented voluntary blackout of thousands of Internet websites was staged in protest of PIPA and SOPA, and Congressional offices were deluged with protesting e-mails and phone calls.
* On Thursday, January 19 the largest criminal copyright indictment ever leveled against an online provider was brought against the cyberlocker service Megaupload.com. Seven individuals were charged with conspiracy, money laundering, and direct infringement and face up to 20 years imprisonment each. The website was seized and operationally shuttered, its landing page replaced with a notice stating “This domain name associated with the website megaupload.com has been seized pursuant to an order issued by a U.S. District Court.” Dozens of servers located in the State of Virginia hosting files placed by Megaupload users came under the possession and scrutiny of the FBI.
* On Friday, January 20 Senate Majority Leader Harry Reid and House Judiciary Committee Chairman Lamar Smith announced that consideration of PIPA and SOPA would be suspended until further notice. Netizens immediately proclaimed a major victory by a new Internet-based citizens’ movement using online protests to counter traditional inside-the-Beltway lobbying tactics.

Yet no one involved with Congressional interaction on either side of the issue believes it has been sidetracked for long, and “Hollywood” and “Silicon Valley” are both plotting their next moves in this high-stakes game to further define the responsibilities and potential liabilities – both civil and criminal - of Internet intermediaries that provide technologies with both legitimate and infringing uses. The resolution of this dispute will determine the ability of Internet services to move to “the cloud” and the responsibilities and restrictions that will be placed on cloud service providers. Further, the White House policy statement on anti-piracy legislation was almost surely informed by advance knowledge of the impending MegaBust and must be evaluated as one part of an overall Administration strategy that is transitioning from domain seizures to major criminal enforcement efforts.

This article will not opine on the merits of the case against Megaupload.com or its probable outcome – that is a matter for the criminal courts to determine, if and when the arrested principals of the company are extradited to stand trial. Under U.S. law they are of course entitled to a presumption of innocence and the government is required to prove the elements of the charges against them beyond a reasonable doubt.

**It is however the viewpoint of this article that the Megaupload indictment will likely be seen in the long run as having a more significant impact on Internet business models and innovation than the withdrawal of PIPA and SOPA – and this would be the case even if those bills had been enacted in some combined form.**

That is because those bills, problematic as they were, created new forms of civil copyright enforcement – blocking of infringing foreign websites by both search engines and ISPs, and termination of third party payment and ad services for both foreign and domestic infringing websites. Such remedies might of course curtail a website’s income and even lead to its demise, as well as to executive and worker unemployment and investor monetary losses. But they would not threaten executives and investors with involuntary, decades-long incarceration in Club Fed.

**Expanding criminal prosecutions to an area that has primarily been the subject of civil litigation is a major step; Washington, DC criminal defense attorney Jeff Ifrah opined that the government's criminal prosecution is "more suitable to the type of steps that the government takes against an organized-crime enterprise dedicated to murder, theft and racketeering." George Washington University Law Professor Orin Kerr observed after the arrests and seizures that “The goal of the Megaupload indictment is to push and prod other companies to take copyright infringement more seriously.”**

**That is undoubtedly true. But it is one thing to take copyright seriously, and another to have no clear idea of where criminal conduct commences. Detailed review of the 72-page indictment against Megaupload reveals no clear “line in the sand” separating civil from criminal copyright infringement or indicating when and against whom the government will level its most potent enforcement weapon. Yochai Benkler, Professor of Entrepreneurial Legal Studies at Harvard and faculty co-director of its Berkman Center for Internet and Society, characterized the MegaBust as “aggressive”, adding:**

***What is a surprise is how aggressive the move is, how much it uses extensions of criminal law enforcement and copyright liability to go after and seize assets and people in anticipation of a full trial. When a new technology comes along [...] and destabilizes the way the industries have always made money, the first gut response throughout the 20th century has been; let’s shut down this technology. What’s chilling here is that a company can be served with a one-sided indictment that lists a whole set of quasi-legitimate and legitimate technological components that lots of other companies use. By the time it will be finished litigating whether that’s enough or not it is dead, because these procedures for forfeiture during the trial will kill the company.***

**This very uncertainty may indeed be a primary goal of the prosecution, as every online company subject to U.S. jurisdiction offering services that have both legitimate and non-infringing uses now needs to question whether it must implement limitations and monitoring regimes lest government agents arrive at its door. This combination of potential criminal prosecution and an indistinct demarcation of what will trigger it may well result in much more “voluntary” curbing of the activities that irk Hollywood than new civil legislation, however amorphous its definitions and onerous its provisions might be, but such actions will come at a significant cost to U.S. technological leadership.**

**The Megaupload prosecution also raises significant questions about the treatment of user data entrusted to cloud and cyberlocker services, and whether non-infringing data can be subject to police seizure and search at the very time it is rendered inaccessible to its owners. The answers to these questions may well determine whether the forecast migration to Internet “cloud” services actually occurs – and, if it does, what proportion of activity is sited outside the U.S. to avoid potential prosecutions modeled on the MegaBust.**

**It also remains to be seen how the indictment will affect the fate and scope of legislation, like PIPA/SOPA, aimed at “rogue foreign websites” -- even as the specter of criminal prosecution and non-legislative efforts, such as trade agreements and enforcement, become greater factors in the ongoing struggle over the proper balance between IP enforcement and digital innovation.**

**Let us now address some of the Mega-questions raised by the MegaBust---**

**What does the indictment tell us about the current line between civil and criminal liability?**

We have carefully reviewed the full 72-page indictment against the alleged Mega Conspiracy to attempt to discern what separates its activities from those of other Internet intermediaries who have faced only civil litigation, or none at all. The dividing line is hazy.

The opening question is whether the $monetary value or impact of the alleged piracy is a critical factor determining criminal prosecution? While the alleged copyright infringement was certainly of a commercial scale, the monetary rewards of Megaupload’s alleged commercial infringement turn out to be relatively paltry in the big scheme of things. The indictment alleges that Megaupload took in a total of $175 million in revenues from 2005 through the Bust, of which $150 million was from user subscriptions and $25 million was from advertising. (Note: That claimed division of income sources is undercut by one e-mail exchange cited in the indictment, in which a company official, reacting to a news story that the Recording Industry Association of America (RIAA) was seeking to have MasterCard terminate payment services to Megaupload, responded, “We are watching the unfolding events with interest, but as the vast majority of our revenue is coming from advertising, the effect on our business will be limited.”) That is a gross revenue figure, and Megaupload had annual costs for bandwidth and storage that ran into the $millions – the money laundering portion of the indictment characterizes the $13 million paid to Carpathia Hosting for U.S. server storage, and the $65 million total paid for hosting services globally, as an (questionable) example of that alleged offense, but it’s indicative of the significant operational costs that Megaupload shouldered. The indictment also fails to break out what percentage of revenues may have been gathered from the perfectly legal sale of storage for non-infringing data, a fact that will perhaps be brought out at trial by the defense.

In any event, this was a website excoriated by Hollywood as one of the leading Internet “pirates”, a website listed in the Office of U.S. Trade Representative’s (USTR) December 2011 “Notorious Markets” report. Yet its annual gross revenues averaged $35 million, from which one must deduct operational costs and break out the portion paid for non-infringing storage to arrive at actual profits derived from alleged infringing activities. What’s also ironic is that despite Hollywood’s refrain that it “can’t compete with free”, Megaupload apparently found a way to make the majority of its revenues from subscriptions – its services were not free to its most devoted users and, if the indictment is to be believed, Megaupload found a way to get them to pay for content they probably could have obtained for free elsewhere on the Internet. The indictment also claims, without documentation, that Megaupload cost the content industry $500 million but that too seems paltry for one of the largest supposed “pirate” enterprises, given entertainment and software industry claims of tens of $billions in annual losses to online infringement.

Most of the indictment consists of conspiracy counts, and the single count alleging direct infringement is likewise paltry. The only direct infringement alleged in the indictment consists of:

* Willful infringing distribution of the motion picture “Taken” before it was released commercially, and
* Infringement of ten or more unidentified copyrighted works that had a total retail value exceeding $2,500.

Although one assumes that more detailed evidence of specific willful infringement will surface at trial, all of the conspiracy counts are presently built upon this rather slender foundation in combination with the claim that Megaupload knowingly paid third parties for infringing content.

Certainly the most damning allegations in the conspiracy portions of the indictment are of those payments, and that the indicted principals had full and detailed (not just general) knowledge of the infringement and even sought out specific content desired by users. The indictment attempts to segregate this from legitimate activity by stating “In contrast to legitimate Internet distributors of copyrighted content, Megaupload.com does not make any significant payments to the copyright owners of the many thousands of works that are willfully reproduced and distributed on the Mega Sites each and every day.” But the DMCA does not require such payments to qualify for an intermediary safe harbor, only an effective notice-and-takedown system -- and many other providers of cyberlocker services do not make such payments notwithstanding that users can utilize their systems for unauthorized distributions of copyrighted materials.

Many of the charges in the indictment describe activity that is common to a broad array of websites. As noted by Professor James Grimmelmann of New York Law School:

*If proven at trial, there's easily enough in the indictment to prove criminal copyright infringement many times over. But much of what the indictment details are legitimate business strategies many websites use to increase their traffic and revenues: offering premium subscriptions, running ads, rewarding active users. I hope that if this case goes to trial and results in convictions, that the court will be careful in sorting out just what Megaupload did that crossed the line of criminality.*

We share that hope, but doubt that it will be adequately fulfilled. And that is a major problem – because such secondary allegations of evidence of infringing intent in this case, if the prosecution is successful in obtaining convictions and the court does not specifically reject them, could well be cited as primary evidence of criminal conduct in future prosecutions of other Internet intermediary companies.

Some of those common business strategies cited in the indictment include:

* Deleting files that hadn’t been downloaded for some time – but this is commonly done by cyberlocker services that primarily provide short-term storage of files too large to send as e-mail attachments.
* Removing only links to files, rather than the entire file. But many storage services engage in such de-duplication practices, in which identical files that have been uploaded (e.g., the latest Lady Gaga single) are identified and just one master copy retained, with multiple users getting different links to it. But if a user has purchased a digital music file or has ripped the file from a purchased CD he has as much right to store it on an online server as on his home computer or iPod, and deleting the entire file would deprive that individual of his non-infringing access to content he has paid for and owns. (The indictment’s recitation of the fact that Megaupload removed files, and not just links, for child pornography and “terrorism propaganda videos” is an apples and oranges comparison, as child porn is per se criminal content that no one has a right to view, and terrorism videos constitute content designed to promote and facilitate violent criminal acts.)

The indictment also listed actions that would seem to constitute evidence that Megaupload was not willfully facilitating infringement, or at least was trying to clean up its act:

* Megaupload removed the search feature on its website, which had previously been of assistance to those looking for infringing content. The indictment alleges that this was done to disguise the company’s willful infringement, much of which was purportedly facilitated by other “linking” websites operated by unrelated third parties. But if the search feature had not been removed, wouldn’t that have been cited as evidence of facilitating infringement? Similarly, the indictment notes that “browsing the front page of Megavideo.com does not show any obviously infringing copies of any copyrighted works; instead, the page contains videos of news stories, user generated videos, and general Internet videos in a manner substantially similar to Youtube.com”, but then cites “the most-viewed videos in the Entertainment category on Megavideo.com… has at times revealed a number of infringing copies of copyrighted works that are available from Mega Conspiracy-controlled servers” as evidence of knowing facilitation of commercial infringement.
* Megaupload provided major content owners with means to directly remove links to infringing content without filing a DMCA takedown notice – its “trusted partners” granted such privileges included Microsoft, Sony, BBC, IFPI, and takedown processor DtecNet. When Time Warner requested an increase in its limit of removing 2,500 links per day Megaupload approved a doubling to 5,000 – and the indictment cites that limitation, for a removal practice not required by law, as evidence of infringing intent. (Megaupload maintained a U.S. agent for DMCA complaints, and indeed it had a link to DMCA complaint filing on every page of its website. Also, despite its lack of direct corporate nexus with the U.S., it did respond to legal actions brought against it – late in 2011 it settled a copyright infringement complaint brought against it in California by the litigious pornography provider Perfect 10.) Of significant concern to every Internet intermediary that relies on the DMCA safe harbor is the allegation that “they are willfully infringing copyrights themselves on these systems; have actual knowledge that the materials on their systems are infringing (**or alternatively know facts or circumstances that would make infringing material apparent**)” and “receive a financial benefit directly attributable to copyright-infringing activity **where the provider can control that activity**” (Emphasis added) This implies that the mere knowledge of facts and circumstances evidencing some degree of infringement by a website operator and a failure to undertake steps to control the activity can be cited as evidence of criminal intent (although the indictment fails to state how a website using user-generated content or providing cyberlocker services might exercise such control, beyond DMCA compliance).
* The company had approached Universal Music to discuss potential licensing and was told that to be considered it must implement "proactive fingerprint filtering to ensure that there is no infringing music content hosted on its service; proactive text filtering for pre-release titles that may not appear in fingerprint databases at an early stage; terminate the accounts of users that repeatedly infringe copyright; limit the number of possible downloads from each file; process right holder take down notices faster and more efficiently." Other than the DMCA’s requirement for termination of repeat infringers and for “expeditious” takedowns (generally regarded as within 24 hours, although some web hosting services believe that removal within 72 hours meets the standard), none of these actions are required by U.S. law -- so it is not at all clear why any failure to acquiesce to demands made during such contractual licensing discussions constitute evidence of ill intent. And Megaupload contended that all DMCA takedown requests were accommodated within 24 hours, and that it had in fact terminated the accounts of more than 120,000 repeat infringers.

The gist of the prosecution’s theory seems to be that many of the actions taken by Megaupload to ostensibly reduce infringing use of its system were an elaborate ruse and actually constitute proof of criminal subterfuge. Yet, given how many Internet services have “come in from the cold” after initially aggregating users through at least tolerance of infringement, is that path now closed off? Ironically, the USTR’s December 2011 “Notorious Markets” report accords credit for such remedial action, stating:

*Following their inclusion in the February 2011 Notorious Markets List, several markets took action to address the widespread availability of pirated or counterfeit goods. USTR commends these efforts, and encourages these and other markets to continue their efforts to curb illicit activity. Examples of positive action at markets that USTR identified in the February 2011 list include the Chinese website,* ***Baidu,*** *identified in the Notorious Markets List for several years, which entered into a landmark licensing agreement with U.S. and other rights holders from the recording industry… These markets are no longer included in the Notorious Markets List. The positive efforts undertaken at those markets will benefit U.S. and other IP right holders.*

Finally, there are some allegations that seem to make no sense at all. Among them is the charge that one instance of money laundering consisted of "on or about November 10, 2011, a member of the Mega Conspiracy made a transfer of $185,000 to further an advertising campaign for Megaupload.com involved a musical recording and a video." This was in fact a video that consisted of a host of Grammy-award winning musicians and other celebrities extolling the virtues of Megaupload for collaborative work on their songs and videos -- the very same video that led the company to sue Universal Music when it subsequently removed it from YouTube.

Some have speculated that the MegaBust took place because Megaupload was about to relaunch its MegaBox website to compete against other licensed online music services -- and that it was actively contracting with major music artists to be part of a service that would put ninety percent of revenues into their pockets, a business model that was extremely threatening to the major record labels. Late in 2011, Megaupload Chairman Kim Dotcom stated, ““You can expect several Megabox announcements next year including exclusive deals with artists who are eager to depart from outdated business models…They [the major labels] don't understand that the rip-off days are over. Artists are more educated than ever about how they are getting ripped off and how the big labels only look after themselves." However, the investigation of the company’s activities had started two years prior and there is no way that it could have envisioned such a development. Whether it generated anxiety in Hollywood that was communicated to Washington is unknown.

One of the most curious recitations in the indictment is this: “On or about February 11, 2007, VAN DER KOLK sent an e-mail to ORTMANN indicating that ‘Kim really wants to copy YouTube one to one.’” The indictment also states, “members of the Conspiracy reproduced copyrighted works directly from third-party websites, including from YouTube.com, to make them available for reproduction and distribution on Megavideo.com”. Megaupload certainly had no right to copy user generated content placed on YouTube. But to the extent that it was copying infringing material why is it a criminal enterprise while YouTube has become a treasured piece of contemporary Americana – indeed, a service regularly used by members of Congress for constituent communications and campaign videos? (And, we might add, at least to this point YouTube has prevailed in the civil copyright infringement case brought against it by Viacom, much of which promotes theories of civil liability that closely resemble the purported evidence of willful criminal activity outlined in the Megaupload indictment.)

A recent New Yorker profile of YouTube’s evolution makes one wonder if the “YouTube Conspiracy” might not have been criminally targeted if this enforcement tactic was being employed when it launched in 2005, especially since e-mails between its principals indicated a deliberate toleration of infringing content to build traffic – e-mails that bear a distinct resemblance to some of those reproduced in the Megaupload indictment:

*On June 20th, Karim wrote in an e-mail to Chen and Hurley, “If we want to sign up lots of users who keep coming back, we have to target the people who will never upload a video in their life. And those are really valuable because they spend time watching.” What the watchers wanted was music videos, skits from “Saturday Night Live,” and episodes of “South Park”—professional content. “And if they watch, then it’s just like TV, which means lots of value,” Karim added.*

*In e-mails that later became the centerpiece of a billion-dollar copyright-infringement suit brought by Viacom against YouTube, in 2007, both Karim and Chen advocated a laissez-faire response toward copyrighted content. If the content owners asked YouTube to take a video down, the site would comply; otherwise, the founders would leave it. Hurley presciently wrote, “OK man, save your meal money for some lawsuits.” But he, too, went along with the relaxed approach.*

*In June, the site incorporated a number of new features, including the ability to embed YouTube videos in other sites and links between videos, and traffic began to pick up. By December, YouTube had several million views a day. That month, “Lazy Sunday,” a skit from “Saturday Night Live,” in which Andy Samberg and Chris Parnell rap about eating cupcakes from Magnolia Bakery and going to a Sunday matinée of “The Chronicles of Narnia,” was posted on YouTube, and viewed more than five million times before it was removed at NBC Universal’s request.*

*In October, 2006, Google bought YouTube, for $1.65 billion… Within a year, Google had tamed the Wild West of copyright infringement that characterized YouTube’s pioneer days, both through licensing deals with major content providers and through a content-management program, called Content ID, that alerted copyright holders automatically whenever any part of their content went up on YouTube. Owners can choose to remove the content, sell ads against it and share the money with YouTube, or use it as a promotional tool. Content ID generates a third of YouTube’s revenue. (In June, 2010, Louis Stanton, the judge in the long-running Viacom v. YouTube case, granted summary judgment to YouTube. Viacom is appealing that ruling, and a decision is expected soon.)*

As described, YouTube’s “laissez-faire response” paid off with a $1.65 billion sale – a lot bigger payday than Megaupload netted from its alleged infringement toleration. And Google has since established a system by which content owners can share in the monetization of their infringed content – imagine if Megaupload had tried that.

Notwithstanding the sidetracking of SOPA and PIPA, Google remains a principal target of many content industry complaints about “profiting from piracy”. A January 2012 study released by the International Federation of the Phonographic Industry (IFPI) contends that when an artist’s name was entered in combination with “mp3” infringing results from Google averaged substantially higher than on the Yahoo! And Bing search engines.

Of course, Google has been accused of worse – and has paid the price. A January 25, 2012 front page story in the Wall Street Journal detailed how a Federal task force was actually preparing criminal charges against the company and its executives in mid-2009 for knowingly accepting ads from illegal pharmacies promoting not just fake drugs but real doses of human growth hormone, steroids, weight-loss pills, and controlled narcotics such as oxycodone. The story relates that the task force had served grand jury subpoenas and collected more than 4 million pages of evidence; one U.S. Attorney is quoted stating that now-CEO Larry Page “knew what was going on” and that “this was a corporate decision to engage in this conduct”. Google retained former Clinton Administration Deputy U.S. Attorney Jamie Gorelick, who subsequently engaged in two years of negotiations leading to a $500 million settlement – the amount equaling Google’s own profits from the ads plus what the Feds claimed were the revenues generated to the illegal pharmacies.

Contrasting the two cases – Megaupload’s alleged infringing conduct which allegedly generated $175 million in revenues and cost the entertainment industry $500 million (although claims of revenue losses from online infringement are notoriously and endlessly debatable) versus Google’s toleration of illegal Rx ads which led to a $500 million forfeiture – one is struck by the key role played by prosecutorial discretion in such investigations. Is the criminal indictment versus civil forfeiture explained by the fact that one company was based in the Far East while the other is central to the Silicon Valley ecosystem and the current state of the Internet? By the ability to portray Megaupload CEO Kim Dotcom as a high-living “pirate” – with a fleet of expensive autos sporting such ill-considered vanity plates as "MAFIA," "STONED," "HACKER, "EVIL," and—(admission against interest?) “GUILTY" -- while Eric Schmidt cultivates a more sedate public persona? Or that one company had no presence in Washington while the other is closely tied to the current Administration? It’s worth pondering, even though we’re unlikely to ever know the full stories behind the very different treatments.

In any event, on February 9 the Wall Street Journal reported that Google plans to wade into the cyberlocker space in a major way with a new service named Drive that will allow users to store large files in the cloud and provide access links to others via e-mail, and that will be accessible for storage and access/download from both computers and mobile devices. The new service will directly challenge such existing providers as Dropbox Inc., Apple’s iCloud, and Box.net; Amazon’s Web Services in turn provides the raw storage capability that backs many of these services. The Drive service will reportedly be free except for those users seeking very large amounts of storage; and will provide for the cloud storage of photos, documents, and music and video files. While such services are incredibly useful for many non-infringing uses they can also be readily used by those seeking to share infringing materials, and their growth is guaranteed to generate new calls from Hollywood for placing responsibilities on Internet intermediaries that go considerably beyond the DMCA’s notice-and-takedown provisions. And the MegaBust has cast a cloud over “the Cloud” itself; one Megaupload user who stored HD family videos on it lamented after the takedown, “Now I find it hard to trust in any service, because Dropbox or any of the other competitors could be brought down by the FBI."

Dropbox, for its part, is one of the hottest startups to emerge from Silicon Valley in recent years. Founded in 2007, it raised an eye-popping $250 million in venture capital in September 2011, was voted “startup of the year” at the January 2012 Crunchies Awards, and currently has more than 50 million users. The Dropbox technology is a Hollywood nightmare – dragging any file into a Dropbox folder placed on any computer, tablet, smart phone, or other device owned by a user causes it to automatically appear on every other user device. In discussing the company’s vision, Sujay Jaswa, VP of Business Development and Sales, stated, “The cool thing about the Internet is that everything is going to be connected. But it’s less interesting if all your stuff is not there and you’re not able to share it.” Another company official noted that, “Now people are working across many geographic regions and we’re in a much different place than we were five or ten years ago.” Vast reductions in storage costs allow Dropbox to offer its basic service, 2 GB of storage, for free – and 2 GB accommodates a very large number of files.

In short, a major goal of “the Cloud” is the facilitation of friction-free global file-sharing, and the more that goal is attained the more difficult it will be to halt “piracy”.

**What Rights do Users of Cyberlocker and Cloud Services Have When Their Provider is Busted?**

None at present, apparently. Whatever rights might have been embodied in the customer terms of service accepted by Megaupload users (or, potentially, those of any other cyberlocker or cloud service) went by the wayside when the FBI shut down the website and seized the storage servers. While the percentage of Megaupload users who employed it for non-infringing purposes cannot be known, it appears to have been widely used by musicians and filmmakers, software coders, and a wide variety of individuals and businesses that employed the service to store, share, collaborate on, and distribute their own works. Megaupload claimed that 5 out of 6 Fortune 500 companies used its storage facilities. Its leased servers stored 12 billion unique files, and its 50 million average daily users transferred about 800 files per second, generating about four percent of global daily Internet traffic (these figures give some idea of the difficulties that would be encountered in designing, much less implementing, and real-time monitoring service having the goal of culling out infringing file-sharing from perfectly legitimate use). Indeed, as noted, a group of world famous musicians had recorded a video invoking the virtues of Megaupload as a collaborative creative tool late in 2011, and the company had initiated litigation against Universal Music for what it claimed was an unauthorized and illicit takedown of the video from YouTube shortly before the bust went down.

On January 30 a letter from U.S. Attorneys involved in the case indicated that the data of more than 180 million total Megaupload users might be erased within days from leased servers owned and operated by Carpathia Hosting and Cogent Communications, stating, "It is our understanding that the hosting companies may begin deleting the contents of the servers beginning as early as 2 February.” The letter also revealed that the US "copied selected data" but did not remove any servers from the premises of either company, and that the data "remains at the premises controlled by, and currently under the control of Carpathia and Cogent. Should the defendants wish to obtain independent access... that issue must be resolved directly with Cogent or Carpathia."

Of course, while Megaupload may well need the data preserved to prepare its defense it has no means of paying for continued storage given the government’s seizure of its assets. And access by its former users is an entirely different matter. At the time the U.S. letter was issued, Megaupload attorney Ira Rothken stated, "We're cautiously optimistic at this point that--because the United States, as well as Megaupload, should have a common desire to protect consumers--this type of agreement will get done."

But Justice Department officials expressed little empathy, responding to one press inquiry as follows:

*This is still an ongoing matter. It is important to note that Megaupload clearly warned users to keep copies of any files they uploaded. Megaupload.com expressly informed users through its Frequently Asked Questions ('FAQs') and its Terms of Service that users have no proprietary interest in any of the files on Megaupload’s servers, they assume the full risk of complete loss or unavailability of their data, and that Megaupload can terminate site operations without prior notice.*

Subsequently, the two hosting companies announced that they would preserve the data for an additional two weeks. The Electronic Frontier Foundation (EFF) then joined with Carpathia to help users retrieve their data, establishing the website [megaretrieval.com](http://www.megaretrieval.com/) to facilitate the effort. On the website, EFF states:

*EFF is troubled that so many lawful users of Megaupload.com had their property taken from them without warning and that the government has taken no steps to help them. We think it's important that these users have their voices heard as this process moves forward.*

For its part, a Carpathia official is quoted on the website:

*We have no immediate plans to reprovision some or all of the Megaupload servers. This means that there is no imminent data loss for Megaupload customers. If this situation changes, we will post a notice at least 7 days in advance of reprovisioning any Megaupload servers at* [***www.Carpathia.com***](http://www.carpathia.com) *and* [***www.MegaRetrieval.com***](http://www.megaretrieval.com).

Pirate Parties in Europe also stated their intent to bring complaints to U.S. authorities over the loss of access, and possible loss of their files, suffered by EU users, although no such activities have been commenced.

While not directly on topic, dicta contained in the U.S. Supreme Court’s unanimous January 23, 2012 decision in U.S. v. Jones, in which it declared that the attachment of a GPS tracking device to a suspected drug trafficker’s auto and subsequent monitoring of his movements for 28 days, violated Fourth Amendment protections against “unreasonable searches and seizures”, seems nonetheless relevant to the issue of search and seizure of files entrusted to cyberlocker services.

The majority opinion based its decision on a narrow extension of the common law’s trespass doctrine and the physical attachment of the GPS device to the auto, leading a concurring minority to complain that the ruling failed to flesh out what constituted reasonable expectations of privacy in the Internet age, much less whether such tracking would be permissible if it did not require a physical device (say, for example, if the police simply monitored the GPS device built into many modern autos, and embodied in nearly every smart phone).

Justice Sotomayor, for example, opined:

*More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expecta­tion of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks… I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.*

Likewise, Justice Alito, for himself and three other Justices, added this in regard to the “expectation of privacy” test developed in relevant case law:

*Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce sig­nificant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this develop­ment as inevitable.*

*On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions.*

Indeed, unless one of Megaupload’s users is subsequently indicted on charges based on evidence gathered by law enforcement authorities after they seized and examined the company’s servers, there will be no opportunity for the judicial system to shed any light on what reasonable expectations of privacy users of cyberlockers and broader Cloud services – both examples of “dramatic technological change” - may have when they share their personal and business data in this manner. There would be little doubt that a warrant would need to be obtained, based upon probable cause, if the police wished to search the hard drive of a computer or other storage device located in a suspect’s home or on his person – but it is not at all clear that any such requirements apply when the very same data is stored on servers owned by or operated on behalf of a third party cyberlocker service.

**In the wake of the MegaBust, some near term certainty is required in regard to what access legitimate, non-infringing users of these services will have to their data when law enforcement authorities shutter the website and seize the servers based upon the allegedly infringing conduct of others, and what assurances they have that the police will not go on a fishing expedition and rifle through their data once those servers are in its possession. Such certainty cannot be provided by the courts in a timely and comprehensive matter. This is exactly the sort of policy issue that Congress is uniquely positioned to investigate and then legislate upon.**

**What is the Short and Long Term Impact on Cyberlocker and Cloud Computing Services?**

For our purposes we’ll consider cyberlocker services to be a subset of “the Cloud”. All cyberlocker services let users store files on remote servers owned or leased by the locker company. The services vary by cost (with some providing limited free, ad-supported storage), maximum file size, total storage allowance, and time that files will be retained. Most allow some sharing, sometimes by links as well as by e-mail. Full spectrum cloud services provide data storage but also move software applications off the desktop or laptop and into the cloud. While some corporations have established private, internal services of this type, most individuals and small businesses must choose from among those that cater to the general public and are far more likely to be a potential target for prosecution.

In choosing which service to use, a potential customer must now consider whether it may be targeted for willful and knowing facilitation of infringing activities and shut down like Megaupload. Unfortunately, the more utility a service provides in terms of maximum file and storage allocation, and ability to share and collaborate, the more it can also be used for infringing activities. Users may reduce their risk somewhat by choosing a service that is offered by a large company with established reputation (e.g., Amazon or Microsoft), that caters primarily to business users, or that does not permit public sharing. But none of these factors is an ironclad guarantee against unanticipated prosecutorial shutdown, and critical files should always be retained on a home or office backup drive.

In any event, the number of services from which to choose and their functionality appear to be in at least temporary decline post-MegaBust. The FileSonic and FileServe services disabled all file-sharing within days after, and Upload.to cut off all access from U.S. users (notwithstanding the domain being hosted on the country code TLD of the Pacific Ocean nation of Tonga). Hong Kong-based Filesonic, one of the Internet’s top 10 file-sharing sites, terminated its affiliate rewards program. FileJungle and UploadStation disabled all third party downloads, and UploadBox and x7.to shut down all operations.

Curiously, Rapidshare, a prominent German cyberlocker company with a business model, and user capabilities and features, quire similar to Megaupload, and which was included on the “2010 International Piracy Watch List” issued by the Congressional International Anti-Piracy Caucus, has made no changes to its service. Company officials stated, "The Megaupload raid and the arrests have nothing to do with the business model of file storage. They have everything to do with the alleged misconduct of individuals." While Rapidshare has ended past incentive programs and claims to have banned many infringing users (changes that Megaupload claimed to have made as well), the RIAA claims that it provided the company with 200,000 DMCA takedown notices in 2011. Most interestingly, one count in the Megaupload indictment alleges that a developer used by the company copied “The Matrix” soundtrack from Rapidshare in March 2011 and subsequently uploaded it to a website controlled by Megaupload. A January 30, 2012 story in the Wall Street Journal reported that Rapidshare has expended $630,000 on Washington lobbying activities since 2010.

**Regardless of whether future cyberlocker busts come down or who is targeted, non-U.S. users of such services may well decide to avoid any such services that have any nexus with the U.S. – be it registry, registrar, headquarters, server hosting, or anything else that could lead to FBI seizure and search. Such avoidance of U.S. providers need not be based in any infringing activity by those users but simply a desire to avoid the possibility of loss of access as well as police review of one’s personal or business data residing on seized servers. While the U.S. web hosting industry should not facilitate willful infringement, neither should it be placed at competitive disadvantage by an uncertain legal environment.**

**Are We Likely to See Additional Criminal Copyright Actions of this Scale?**

It’s too soon to say whether the Megaupload bust will be a one-off or the start of a new line of criminal copyright enforcement cases. Certainly, if one intent of the prosecution is to create a FUD climate (fear, uncertainty and doubt) in which online entities offering cyberlocker and other services capable of infringing uses police their own websites and offer broad access and intervention capabilities to content entities – that is, to take “voluntary” steps that go considerably beyond notice-and-takedown duties under the DMCA –there will probably need to be additional cases brought against companies which are more mainline and less outlaw in public perception than Megaupload.

The U.S Attorney who brought this case is the former head of anti-piracy activities for the Business Software Alliance, but he is just one of many former officials with the content industries and their trade associations and law firms who have been brought into the Obama Administration and may have a similar mindset. There may well be some delay before additional indictments are filed; given that “hard cases make bad law” there may be a desire to test and enshrine the legal theories underlying the indictment in this colorful case before prosecutions are leveled at companies with more mainstream images and business models.

But it’s not as if the use of cyberlocker services has ended – their users (both infringing and non) have simply shifted to other providers. Reportedly, most of Megaupload’s traffic quickly shifted to such services as Filefactory, Depositfiles, Hotfile.com, Filepost.com, Hulkshare.com, and Uploading.com – and even 4Shared, a cyberlocker with reportedly twice the storage capacity of Megaupload. Now each of these providers must be scrutinized individually by potential users regarding their policies and practices, as well as their connections with U.S. users and businesses – but it would be surprising if one or more of them wasn’t a potential target for future DOJ action.

If domain seizures are any precedent, then there certainly will be more Mega-style criminal prosecutions. Certainly, no one anticipated that President Bush’s signing of the PRO-IP Act in 2008 would lead to sweeping domain seizures as a new IP enforcement too. For example, on February 2, 2012 the Immigration and Customs Enforcement Division (ICE) of the Department of Homeland Security (DHS) announced the seizure of 307 domains – 291 of which were alleged to be distributing counterfeit NFL merchandise, and 16 of which were alleged to be streaming infringing broadcasts of sports events -- in “Operation Fake Sweep”. This Super Bowl-related enforcement was the latest act in “Operation In Our Sites”, which has seized a total of 669 domains since its initiation in June 2010.

That PRO-IP Act also created the position of White House Intellectual Property Enforcement Coordinator, otherwise known as the “IP Czar”. That position is currently held by Victoria Espinel, who was the lead signatory of the January 14th White House statement indicating that PIPA and SOPA were not acceptable in their current forms. That White House policy statement must be evaluated in light of the subsequent MegaBust – as the indictment was filed with the Clerk of the U.S. District Court in Alexandria, VA on January 5, 2012, a full two weeks before arrests were executed and the domain and servers seized. Ms. Espinel surely had advance knowledge that the enforcement actions were imminent. While we can only speculate as to what if any political calculations were factored into the White House position, it is a Presidential election year and it was becoming increasingly apparent that the PIPA/SOPA debate, much less White House support for the legislation, could jeopardize the enthusiasm of the left wing blogosphere – which had been indispensable in stoking enthusiasm for the President’s 2008 victory – and also sour relationships with the entrepreneurs and venture capitalists of Silicon Valley, now being courted as direct and SuperPAC contributors to the President’s re-election campaign. Derailing the bills eliminated those problems, but risked alienating Hollywood, a key part of the Democratic base.

**In this political context the MegaBust sent a strong signal that, while the White House might not be on the same legislative page right now, Federal law enforcement resources would be expended to shut down a website that Hollywood had long excoriated while sending a warning shot across the bow of dozens more providing similar services. Further prosecutions would amplify that message while simultaneously lessening pressure for legislation.**

**Meanwhile, the Administration is moving to impellent the Anti-Counterfeiting Trade Agreement (ACTA) while resisting calls to submit it for Senate ratification, and is pursuing a new Trans-Pacific Partnership (TPP) that would further ratchet forward IP protections and requirements in Pacific Basin trade. And it establishing yet more dedicated anti-counterfeiting/piracy units -- in his January 24th State of the Union Address, President Obama declared:**

***It’s not right when another country lets our movies, music and software be pirated…Tonight, I’m announcing the creation of a Trade Enforcement Unit that will be charged with investigating unfair trading practices in countries like China.***

**The next day, IP Czar Espinel sent that portion of the Address out by e-mail with a cover note stating, “The Administration will continue to aggressively enforce American rights against those who seek to steal the creativity and innovation this nation uses to prosper.”**

**As always, the best motto for evaluating what’s really going on in Washington is “Watch what we do, not what we say.”**

**Is Legislation Targeting “Rogue Foreign Websites” Still Justified?**

On January 25 – six days after the MegaBust -- the Hollywood-aligned “grassroots” group, CreativeAmerica, released a video heavily focused on Megaupload, and making a very flawed case that PIPA and SOPA were still needed, arguing:

*US law enforcement is only permitted to shut down US-based IP addresses. Overseas sites, like Megaupload and Megavideo, and the Swedish-based Pirate Bay, are out of reach.*

Megaupload Chairman Kim Dotcom, currently denied bail and awaiting extradition proceedings in a New Zealand jail, certainly wishes that this claim was correct. But it is not. Aside from the incredibly inept timing of releasing the video after the arrests and website seizure, the claim is also wrong on the facts – Megaupload is and always has been subject to U.S. jurisdiction (and the Pirate Bay has been found guilty by the courts of Sweden).

PIPA and SOPA always defined a domestic website as any in which the registry or registrar is located in the U.S., and Megaupload.com is a .com website. The .com registry is operated by the U.S. Corporation VeriSign under a contract granted by the U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN) and both it and the .com contract are subject to some degree of oversight by the National Telecommunications and Information Administration (NTIA) within the Department of Commerce. In addition, Megaupload maintained about 28 out of its global total of 100 petabytes of data storage capacity through contracts with U.S. web hosting firms, with those physical assets subject to FBI seizure. Hence, while it was headquartered in Hong Kong, and while its Chairman and other senior executives resided in New Zealand, Megaupload had more than enough U.S. nexus to be subject to American law enforcement. (The indictment recounts a July 2010 e-mail exchange regarding the possibility of a domain seizure in which Kim Dotcom asked, “Should we move our domain to another country (Canada or even HK?)” to which an alleged co-conspirator responded, “In case domains are being seized from the registrar, it would be safer to choose a non-US registrar.” This advice was correct but far from complete, as there is no way to fully shield a .com domain from U.S. jurisdiction. It would be ironic indeed if the arrest of Kim Dotcom, formerly Kim Schmitz before a legal name change, caused a migration away from .com websites to avoid potential U.S. prosecution.)

So did the MegaBust reduce overall file-sharing or simply shift more of it away from U.S. providers? The answer appears to be the latter. A new report from DeepField Networks indicates that the offshore shift has already taken place. Global Internet traffic dropped about three percent in the immediate aftermath of the MegaBust. But within twenty-four hours traffic had returned to earlier levels, with file-sharing traffic shifting primarily to Putlocker, NovaMov and MediaFire, all of which have their storage facilities located largely within Europe. In other words, the shutdown did not diminish possible infringing activity but merely shifted traffic from within the U.S. to transatlantic links, in the whack-a-mole fashion we have seen with prior attempts to reduce piracy by targeting specific providers of services that can facilitate it. The original Napster, Kazaa, Grokster, BitTorrent, and now the Pirate Bay have all been shuffled off the cyber-stage with no lasting impact on “piracy”. (Tellingly, while Megaupload accounted for approximately 4 percent of all Internet traffic at its peak, an October 2011 report from Sandvine Networks indicates that file-sharing is eclipsed by streaming as a portion of total Internet traffic. “Real-time entertainment” – including video, TV, but not online gaming – constituted the majority, 53.6 percent, of all traffic crossing the wired North American Internet during 2011, with web browsing second at 16.6 percent and file-sharing third at 14.3 percent. To the extent that Internet streaming is of non-authorized copyrighted material it may also be classified as part of overall online “piracy”. U.S. law currently classifies unauthorized streaming as a potential misdemeanor but a provision of SOPA, and a Senate bill separate from PIPA, propose to make such activity a felony. In the event that such legislation is ever enacted it would not be surprising to see one or more criminal enforcement actions brought against websites subject to U.S. jurisdiction that facilitate the streaming of user-generated content.)

PIPA and SOPA opponents will undoubtedly point to the Megaupload case and say that new law is unnecessary because one of the largest of accused infringing foreign websites was subject to U.S. prosecution. Hollywood and its allies (assuming they start to get their facts straight) will likely reply that such prosecutorial tools are unavailable against websites with no U.S. nexus – that is, both registry and registrar foreign-domiciled, servers and other physical assets likewise offshore, and – the icing on the cake – located in a nation with no extradition treaty with the U.S.

Such a setup is possible now through a country code top level domain (ccTLD). For example, Germany’s .de domain is the largest in the EU, and Germany has no extradition treaty with the U.S. The possibilities will soon multiply exponentially as ICANN begins processing applications under its new generic TLD (gTLD) program, with 1,000 to 1,500 applications expected in the first 2012 round. While many of the applications will be for .brands from major trademark owners and .geos endorsed by cities, regions, and nations, a significant portion may well be for new generic names. While the entertainment industry can be expected to carefully scrutinize any proposal associated with its content (.music, .video, etc.) and to loudly object if it believes it might harbor infringement, other general purpose gTLDs will undoubtedly be approved, and some will choose to locate in places that are quite immune from the reach of U.S. law. (Note: The RIAA and other members of the music industry establishment have just announced their support for a .music applicant that has promised to limit domain availability to card-carrying members of the “accredited global music community” and to implement active policing to detect copyright infringement.)

**Some nations may even aim to become for data security what others have been for banking and taxation – a very safe haven secure from the prying eyes of outside law enforcement except in the most extraordinary circumstances. Cyberlocker and cloud services located in such jurisdictions may well be charged with harboring infringement, but will also be providing a valuable service to companies and individuals desiring the highest level of privacy for their business and personal data files. Data has become a valuable currency in itself – in many instances a far sounder currency than many of the fiat money regimes currently in existence and presently propped up by nervous central bankers.**

**In this evolving environment trade sanctions may become one of the only practical and most effective means of curbing foreign-based infringement, and the approach suggested by the OPEN legislation introduced by Sen. Wyden and Rep. Issa – enforcement of trade agreement IP protection commitments through actions of the Office of U.S. Trade Representative -- may well finds its way into any future bill addressing online infringement. That begs the question of whether any such legislation can be enacted near-term, much less whether its overall thrust is either advisable or effective.**

**Conclusion**

**The general purpose computer is a digital copying machine, and the Internet has fostered a global network of these copy devices. Copyright law developed in a world of scarcity and control, but we now inhabit an age where the marginal cost of reproducing and globally distributing a perfect copyrighted file approaches zero, where the cost of data storage and computer power continues to decline in concert with Moore’s Law, and where the available means of facilitating infringement continue to multiply. For example, the price of storing 1 gigabyte of data fell from $20 in 2000 to 10 cents in 2010 (which means it will likely be less than a penny by mid-decade), the percentage of U.S. homes with broadband connections has gone from less than 30 percent in 2004 to more than 60 percent at present, and the percentage of North American mobile phone users using speedy 3g networks climbed from 20 percent in 2007 to 54 percent in 2011. These trends are inexorable, they increase the demand for and utility of Cloud services, and they emphasize the difficulties of stemming the unauthorized sharing and streaming of copyrighted files. In addition, the same technologies that facilitate infringement boost productivity and can be employed to incredibly useful and legitimate ends, and short of instituting pervasive real-time monitoring regimes that raise free expression and privacy concerns, and greatly reduce efficiency while adding costs, there is no ready way to readily differentiate user activities.**

**The Megaupload indictment signals the beginning of a new chapter in the more than decade-long struggle between content owners and Internet innovators. It may be time to take a deep breath and ask whether the path of criminal prosecutions with indistinct guidelines regarding who will be next to face jail time is one we really wish to go down.**

**And, more broadly, do we really want to institute a cyber-police regime in which globally distributed storage, linking, and search features are all subject to real-time monitoring and reporting in the name of copyright infringement? To a significant extent the anti-PIPA.SOPA protests were a pushback against the cyber-surveillance state that inevitably flows from aggressive online anti-piracy measures. All efforts to stem online piracy other than offering convenient access to content at reasonable prices have failed to date, and there is little reason to believe it will ever be eradicated by stronger laws and tougher prosecutions no matter how far IP law is ratcheted forward.**

**It is standard operating procedure in Washington to “seek common ground”, “split the difference”, and fashion a “win-win solution”. But sometimes no such resolution is possible because the interests – indeed the very viewpoints – of the contesting parties are fundamentally opposed and genuinely irreconcilable. While efforts will undoubtedly be made over coming months to forge a consensus response to “online piracy”, it may prove impossible to simultaneously impose new policies that restrict copying while preserving open technologies that facilitate copying. One must ultimately bend to the other.**

**The Internet blackout staged against PIPA/SOPA and the engagement of millions of Netizens make it most unlikely that any legislation can be enacted prior to the November 2012 elections – indeed, both Hollywood and Silicon Valley probably have an effective veto over any proposal they dislike for the indefinite future. But, just as file-sharing technology routes around obstacles, Hollywood will likely route around Congressional gridlock with an increased push for state-by-state legislation, international trade agreements, and encouragement of additional criminal litigation in the “war on piracy”.**

**But the ‘war on piracy” may, like the “war on drugs”, be ultimately unwinnable – the first because of the nature of the technology, the second because of human nature. Unwinnable wars of this type should be warily evaluated because they can exert a perpetual call on the public purse, with the law enforcement agencies charged with the war able to engage in large-scale enforcement actions at regular intervals that garner favorable headlines and are cited as evidence of progress, but which do little for long to stem overall trends or illicit activity.**

**And all wars extract collateral damage; the MegaBust extracted some on millions of its non-infringing users. The damage inflicted by continuing criminal enforcements of copyright law that use the Megaupload indictment as their foundation may well be to U.S.-based Internet innovation and services, and to associated employment and technology leadership.**

**Certainly, enterprises that are designed to profit primarily from criminal copyright infringement of U.S. IP should not be immune from U.S. law enforcement or trade sanction actions. But the MegaBust is likely to spur such enterprises to strive to eliminate all legal nexus from the U.S., while successive indictments advance evolving legal theories that further blur the lines between civil and criminal infringement. It would seem incumbent for U.S. policymakers to ponder the questions raised by the MegaBust and begin to provide some answers to the Internet industry and its public users as to their rights and responsibilities in the new cloud environment.**

**Indeed, the current copyright debate may just be a precursor to even broader disagreements as new disruptive technologies, such as 3-D printing, pose additional challenges to IP law formulated in an analog world. As Cory Doctorow observed in his recent essay, “Lockdown: The Coming War on General Purpose Computing”:**

***So, our regulators go off, they blithely pass these laws, and they become part of the reality of our technological world. There are, suddenly, numbers that we aren't allowed to write down on the Internet, programs we're not allowed to publish, and all it takes to make legitimate material disappear from the Internet is the mere accusation of copyright infringement. It fails to attain the goal of the regulation, because it doesn't stop people from violating copyright, but it bears a kind of superficial resemblance to copyright enforcement—it satisfies the security syllogism: “something must be done, I am doing something, something has been done." As a result, any failures that arise can be blamed on the idea that the regulation doesn't go far enough, rather than the idea that it was flawed from the outset….******We don't know how to build a general-purpose computer that is capable of running any program except for some program that we don't like, is prohibited by law, or which loses us money. The closest approximation that we have to this is a computer with spyware: a computer on which remote parties set policies without the computer user's knowledge, or over the objection of the computer's owner. Digital rights management always converges on malware…******It may seem like SOPA is the endgame in a long fight over copyright and the Internet, and it may seem that if we defeat SOPA, we'll be well on our way to securing the freedom of PCs and networks. But…this isn't about copyright…The copyright wars are just the beta version of a long coming war on computation. The entertainment industry is just the first belligerents to take up arms, and we tend to think of them as particularly successful…******As we saw in the copyright wars, all attempts at controlling PCs will converge on rootkits, and all attempts at controlling the Internet will converge on surveillance and censorship.***

**Very big things are at stake, including the scope of our liberties in the shared cyber-future.**

***© 2012 by Philip S. Corwin***