Thursday, March 15, 2012

Megaupload indictment leaves everyone guessing

Tony Falzone is the executive director of the Fair Use Project and a lecturer in law at Stanford Law School. As an intellectual property litigator, he has defended artists, writers, publishers, filmmakers, musicians, record labels and video game makers against copyright, trademark, rights of publicity and other intellectual property claims.

Jennifer Stisa Granick is general counsel of entertainment company Worldstar Management LLC and its flagship website worldstarhiphop.com. She is based in San Francisco.

LAST IN A TWO-PART SERIES: Part one appeared on March 14.

The first part of this article outlined the mechanics of the Megaupload website, and the novel questions of criminal inducement on which the government's indictment is premised. Here, we explore two more extensions of existing law on which the indictment is based, and the impact this prosecution is likely to have on Internet innovators and users alike.

In addition to pushing the boundaries of criminal inducement, the government has put itself in the middle of an ongoing debate about the scope of the Digital Millennium Copyright Act (DMCA) safe harbor contained in 17 U.S.C. Section 512(c). Section 512 protects online service providers from liability based on material placed on the site at the direction of a user, so long as the service has no actual or "red flag" knowledge of infringement, does not receive a financial benefit directly attributable to infringement, terminates repeat offenders, registers an agent for receipt of complaints, and obeys a specified notice and take down procedure. Two recent cases have asked whether the operator's general knowledge that infringing activity is occurring on a service is sufficient to eliminate safe harbor protection. Both said no.

In *Viacom v. YouTube*, Viacom International Inc. presented its one billion dollar claim that YouTube Inc., now owned by Google, welcomed copyright-infringing material on its website, that the popularity of these works enhanced defendants' income from advertisements and that such infringing works were rampant, numbering in the "tens of thousands" just of Viacom's property alone. While the claims parallel the allegations of the Megaupload indictment, the Southern District of New York dismissed the case. It

held that the company's general knowledge that the service hosted copyrighted material, even a lot of copyrighted material, did not defeat DMCA safe harbor protection. Rather, the company must have actual or red flag knowledge that particular clips are infringing, and is not otherwise required to review or police uploads. The case is currently on appeal to the 2nd U.S. Circuit Court of Appeals. *Viacom International Inc. v. YouTube Inc.,* 10-3270 (filed Aug. 11, 2010).

The Megaupload indictment raises the stakes while pushing the boundaries of secondary copyright liability beyond current civil law, which is already muddy and unsettled.

The 9th U.S. Circuit Court of Appeals adopted similar reasoning in *UMG v. Shelter Capital*, 2011 DJDAR 18112 (Dec. 12, 2011). There, copyright owners argued that because the video site Veoh offered access to thousands of music videos without obtaining music licenses, and triggered contextual advertising based on the names of artists whose videos were on the site but with whom it had no license, it must have known that the works on its site were infringing, therefore disqualifying it from the safe harbor.

The 9th Circuit rejected this view, holding that "merely hosting a category of copyrightable content, such as music videos, with the general knowledge that one's services could be used to share infringing material, is insufficient to meet the actual knowledge requirement." The available information must be enough by itself to put the service on notice of specific infringing activity.

The government's indictment alleges a wide array of communications that suggest Megaupload and its principals knew there was infringing content available on the site, and even sought it out. But UMG and Viacom had both done likewise in their cases, and that evidence was not enough to show actual or "red flag" knowledge necessary to eliminate safe harbor protection.

Similarly, in both the *UMG* and *YouTube* cases, the copyright owners claimed that the sites obtained an impermissible financial benefit from infringement because they sold advertising against unauthorized content. Again, neither court agreed. As a result, Megaupload's advertising practices should not eliminate its safe harbor protection, either.

Ultimately, whether Megaupload meets the standards required for safe harbor protection may be less important than whether it believed it did. Criminal infringement requires proof of willfulness and the view of the majority of federal courts, including the 4th U.S. Circuit Court of Appeals where this case is pending, is that "willfulness" means a desire to violate a known legal duty. See *RSM v. Herbert*, 466 F.3d 316 (4th Cir. 2006). Did Mega register an agent? Did Mega have a repeat infringer policy? These are all interesting civil questions. But from a criminal law perspective, if Megaupload and its principals believed they met the requirements of the Safe Harbor, then they were not willfully disregarding the law, and cannot be held criminally liable.

The indictment identifies a number of steps Megaupload took that appear designed to reduce rather than induce piracy. At one time, it included a search feature that permitted users to browse for specific files (e.g. search for "Seinfeld" or "Game of Thrones"), but removed that feature. It provided copyright owners with the ability to remove infringing content directly, without submitting a DMCA notice. If true, Megaupload went beyond what is required by the DMCA to obtain a safe harbor from civil suits for monetary harm from infringement. Yet, the government cites removal of

the search feature as an effort to disguise the fact that pirated material was on the site, and the refusal to give copyright owners unlimited takedown rights as further evidence of bad intent. This skepticism creates a damned-if-you-do, damned-if-you-don't conundrum for file sharing sites.

The boundaries of civil liability for contributing to, or inducing, infringement by other people have grown increasingly murky in the face of technological change. Congress designed the DMCA safe harbor to eliminate some of that uncertainty for companies that provide platforms for users to share content and thereby incentivize innovation and investment. An immense amount time and money has been expended litigating the limits of those safe harbors. Until now, the risk of guessing wrong has always been civil liability, not jail time.

This indictment ups the ante, and leaves the DMCA safe harbor looking a lot less safe. A service with substantial non-infringing uses may nevertheless be labeled a criminal enterprise based on customer misuse. New services must worry that email messages will be cited as evidence of intent to induce. Efforts to comply with the DMCA safe harbor may be ignored and programs to combat piracy outside of what the law requires may be critiqued for not having gone far enough. Entrepreneurs and funders are not going to invest their time and money creating new platforms for sharing information if the rules are murky, and guessing wrong means financial ruin and jail time.

Users have still other reasons to worry. Those who use a platform for perfectly legitimate purposes may nonetheless see their data seized by the government (or destroyed forever) based on the unknown conduct of other users. And once data is seized, users are left to wonder what the government will do with it. The privacy rules applicable to seized information are unknown. Searching a computer can expose evidence of unrelated crimes as well as embarrassing private information. Once a warrant is executed and returned, no statutory rule regulates the timing of subsequent electronic examination of that data. Discovered materials may be admissible in court under the plain view doctrine, or under the theory that the user has no expectation of privacy in data she stores with third parties.

Some judges have imposed limits on how computers are searched to try to ensure that investigations involving such troves of data will be conducted as narrowly and with as much respect for non-suspects as possible, particularly after the 9th Circuit advised the safeguard in its ruling in *United States v. Comprehensive Drug Testing*, 545 F.3rd 1106 (2008). But this practice is neither required nor common.

In sum, the Megaupload indictment raises the stakes while pushing the boundaries of secondary copyright liability beyond current civil law, which is already muddy and unsettled. Every innovator and future customer has to guess whether they might be targeted next.

Wednesday, March 14, 2012

Megaupload indictment leaves everyone guessing

Tony Falzone is the executive director of the Fair Use Project and a lecturer in law at Stanford Law School. As an intellectual property litigator, he has defended artists, writers, publishers, filmmakers, musicians, record labels and video game makers against copyright, trademark, rights of publicity and other intellectual property claims.

Jennifer Stisa Granick is general counsel of entertainment company Worldstar Management LLC and its flagship website worldstarhiphop.com. She is based in San Francisco

FIRST IN A TWO-PART SERIES

Days after anti-piracy legislation stalled in Congress, the U.S. Department of Justice coordinated an unprecedented raid on the Hong Kong-based website Megaupload.com. New Zealand law enforcement agents swooped in by helicopter to arrest founder Kim Dotcom at his home outside of Auckland, and seized millions of dollars worth of art, vehicles and real estate. Six other Megaupload employees were also arrested. Meanwhile, the Justice Department seized Megaupload's domain names and the data of at least 50 million users worldwide.

What did Megaupload do to attract a response normally reserved for drug cartels and terrorists? Depending on whom you ask, it was either a cyberlocker that allowed users to store, share and retrieve any manner of data, or a vast conspiracy to facilitate piracy on a worldwide scale. The government's indictment against Megaupload and its principals is premised on several aggressive extensions of copyright law that will make it even harder to identify the line between legitimate hosting services and criminal conduct, while its data seizure leaves millions of users wondering what the government is going to do with their information and whether they will ever get it back.

In some respects, Megaupload was like many other companies that let people store files in the "cloud." It permitted its users to upload a file, and then provided a URL that allowed that user (or anyone else who knew the URL) to access and download the file from any computer connected to the Internet. Any user could upload files up to 2 GB in size and store a total of 200 GB for free. Premium account holders enjoyed unlimited file size and storage capacity, and substantially faster downloading speeds. These large storage limits and fast upload/download speeds made Megaupload an especially

attractive platform for users who worked with large audio and video files. Musicians and software developers used Megaupload to collaborate and to distribute their work, and many others used it to store a wide range of legitimate content like digital photographs, and audio and video files.

The same features that made Megaupload attractive to legitimate users also made it attractive to people who wanted to share copyrighted content without permission. Some of the site's features seemed calculated to exploit that fact. For instance, Megaupload provided financial rewards to users who uploaded popular files. Arguably, this created an incentive for users to upload copyrighted content and distribute the URL widely. Indeed, the government's indictment alleges that one user received more than $55,000 in rewards. In order to monetize download traffic, the company ran advertisements on each download page. It also created another site called Megavideo, which allowed individuals to stream video content directly, or through another site. In either case, the video content was accompanied by advertising served by yet another entity called Megaclick. As a result, the more popular the files were, the more Megaupload earned from subscription fees and advertising.

The grand jury indictment against Megaupload and its principals alleges they were part of a "mega conspiracy" - "a worldwide criminal organization ... engaged in copyright infringement and money laundering on a massive scale." Some of the accusations in the indictment are straightforward. For instance, Megaupload employees allegedly uploaded prerelease movies to the site, including the film "Taken," knowing these uploads were improper. These direct infringements would be clear violations of criminal copyright law. But the heart of the government's case seeks to impose substantial criminal liability for acts of infringement committed by Megaupload users, not the defendants themselves. In doing so, the indictment pushes several aspects of copyright law well past existing boundaries.

The Copyright Act prohibits specific acts of infringement, e.g., reproduction, distribution, public performance and preparation of derivative works. 17 U.S.C. Section 106. Committing these acts becomes a criminal offense if the infringement is willful, and is committed for commercial advantage or financial gain, involves works with a retail value of more than $1000, or prerelease movies or music. 17 U.S.C. Section 506(a)(1); 18 U.S.C. Section 2319. The Copyright Act does not specify any circumstances in which one party is liable for the infringing acts of another. While copyright law has long imposed "secondary liability" on one party for the infringing acts of another, that doctrine is a function of judge-made, not statutory, law.

In general, a party with control over the direct infringer who fails to stop the infringement, or who knows of the infringement and makes a material contribution to it is secondarily liable. Copyright owners have long argued that companies who supply technology that facilitates both legal and illegal copying are liable for the unlawful acts of their customers.

The Supreme Court addressed that question in 1984, in *Sony v. Universal Studios*. In that case, copyright owners contended that a manufacturer of video cassette recorders was liable for infringement based on copies of television shows and sporting events its customers made using the device. The Court rejected that argument, holding that suppliers of technology are not secondarily liable for users' infringement if the device in question is capable of substantial non-infringing uses.

The Supreme Court narrowed this rule in 2005 when it decided *MGM Studios v. Grokster*. In that case, the Court held a defendant providing Internet file-sharing services capable of substantial non-infringing use was nevertheless liable for unlawful copies made by its users where the evidence showed that the company intended to, and took affirmative steps to, induce the infringing conduct.

Cyberlocker services are plainly capable of substantial non-infringing uses; for example, they allow musicians and filmmakers to collaborate on and share their works. The government's indictment, however, lays out a case of inducement under *Grokster*, pointing to emails and other evidence that the principals knew and encouraged infringement by employees and users alike. The interesting question is whether a judge-crafted theory of civil liability developed in 2005 is sufficient to impose criminal liability. No court has decided that issue, but it is presently before the 2nd U.S. Circuit Court of Appeals in *Puerto 80 Projects v. USA*. In that case, Puerto 80 is challenging the seizure of its rojadirecta.com and other domain names based on the fact its sites linked to infringing content.

Puerto 80's lawyers have challenged the government's assertion that criminal liability can be based on judge-made secondary infringement liability theories, including *Grokster*-style inducement. Specifically, they point out that Congress considered and rejected proposed statutes that would have created such liability so the current doctrine must not include criminal inducement liability. To rule otherwise, they contend, would create criminal liability in vague and uncertain circumstances, violating due process of law.