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.