US Perspectives: ISPs In US Face New Copyright Attack

22/12/2011 BY STEVEN SEIDENBERG FOR INTELLECTUAL PROPERTY WATCH — 2 COMMENTS

Print This Post

It is a novel way to attack online copyright infringement. Two music companies have sued an internet service provider, alleging that because the ISP failed to terminate the accounts of repeat infringers, the ISP is guilty of secondary infringement. This lawsuit troubles many copyright experts and its success is far from certain, but the music companies may achieve their aims regardless.

BitTorrent network

The music industry has been fighting online infringement for almost 15 years, with only limited success. Despite litigation campaigns and the enactment of new laws around the world, online infringement remains "a huge problem for the music industry," said Lawrence Iser, a partner in the Southern California law firm of Kinsella Weitzman Iser Kump & Aldisert. "There is still tons of illegal music online."

So the music industry is trying something different. For the last few years, they have been working with ISPs to implement a graduated response system – often called a "six strikes policy." Basically, the copyright owner monitors internet traffic and notifies the ISP when a subscriber's IP address uploads or downloads infringing material. The ISP passes this notice of infringement to the subscriber, along with a warning. If the subscriber continues to infringe, subsequent warnings take on a more severe tone. After repeated warnings, the ISP may impose sanctions, such as temporarily throttling the customer's bandwidth. But no ISP in the US has gone so far as to publicly embrace account termination as a sanction in its graduated response system.

Most of the big ISPs in the US are participating in a graduated response system, but there are exceptions.

Each ISP that has established a graduated response system sets its own rules on what to say to alleged infringers and what (if any) sanctions to impose. Cox Communications is more lenient than most, using a "ten strike policy."

Two music companies thought Cox was being too lenient, so they sued Cox on 26 November. "They didn't go after other ISPs. They picked Cox because it was not implementing what they thought was a reasonable solution," said Jordan A. Sigale, director of *Dunlap Codding*, an Oklahoma law firm.

In the lawsuit, BMG Rights Management and Round Hill Music allege (pdf) that over 200,000 customers of Cox have used BitTorrent to repeatedly upload and download infringing copies of plaintiffs' music. Cox was notified repeatedly about the infringements, but refused to terminate the accounts of the alleged infringers – thus protecting the revenue Cox receives from these allegedly infringing subscribers. As a result of all this, Cox is liable for contributory and vicarious copyright infringement, the suit claims.

No Safe Harbor?

This is a rather unusual lawsuit. The music industry has not previously targeted ISPs, largely because ISPs, like other online service providers, are protected in the US by the Digital Millennium Copyright Act. Section 512 of the DMCA declares that such online providers are not liable for infringements committed by their users, so long as certain conditions are met.

The lawsuit asserts that Cox has fallen out of the DMCA's safe harbors because the company has failed to comply with Section 512(i) of the Act. This provision states the DMCA's safe harbors "shall apply to a service provider only if the service provider … has adopted and reasonably implemented … a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."

But what is a "repeat infringer" for purposes of this statute? Is it someone whom a court has ruled is a repeat infringer, or is it anyone whom a copyright owner asserts is a repeat infringer? Legal experts don't agree on the answer, and the courts have never ruled on this issue.

The lawsuit against Cox could turn on this unresolved issue. Because if only a court can declare someone a repeat infringer, then Cox is not required by Section 512(i) to terminate the accounts of mere alleged infringers. The ISP would thus maintain its safe harbor protection and would not be liable for secondary copyright infringement.

Pros and Cons of Courts

Requiring a court verdict on every repeat infringer would be impractical, according to Iser. "Think about how long it would take to get such an adjudication," he said.

Costs also make going to court impractical. A copyright owner would incur legal costs for subpoenaing the ISP to obtain the name and address of the alleged infringer and for suing that person for infringement. Such costs might not be great in individual cases, but if a copyright owner wants to go after tens of thousands of alleged infringers, the legal fees certainly would be significant.

There would, in addition, be reputation costs. The last time the music industry engaged in a litigation campaign against alleged online infringers, the industry became the object of scorn and derision, as news stories revealed the industry had sued a variety of sympathetic figures, including a 66-year-old grandmother who knew nothing about file-sharing. In the end, the industry dropped the litigation campaign and vowed not to engage in it again.

Going to court would be costly and time-consuming, but it would be unfair to require ISPs to act on anything less than a judicial verdict, according to many legal experts. Because copyright owners' notices of alleged infringement are often wrong.

Copyright owners routinely notify YouTube and other online hosting services of allegedly infringing content, demanding the services take down the identified "infringing" content. However, "it has become very clear that lots and lots of the notices are wrong. How could that be otherwise? The copyright owners are using mechanized processes to send out millions of notices," said Prof. Jessica Litman of University of Michigan Law School.

One problem is that a copyright owner's investigator can't know who uploaded or downloaded an infringing file. The investigator monitoring the internet can know only the IP address where the supposed infringement occurred. "That could be an open WiFi address. It could be a library, hotel, coffee shop or other small business where some customers or others are using BitTorrent," said Sigale. It would be "draconian," he added, to declare that the innocent owner of such an open IP address is a repeat infringer and must be lose all internet access.

Another problem with internet monitoring is that the copyright owner's investigator can't know for sure that any infringement has occurred. What an investigator thinks is infringement may be fair use, an unluckily named file, or an instance of someone else investigating infringement, Sigale noted.

"The complaint comes down to this: We [copyright owners] send emails saying these people are repeat copyright infringers, and the ISP is supposed to take that as gospel truth and shut these people down. That is crazy," said Sigale. "As a copyright lawyer, I think copyright is super-important, but this isn't a question of protecting copyright. This is an attempt to circumvent due process. This is exactly what the DMCA was supposed to prevent."

Mixing Safe Harbors

The plaintiffs in this case are conflating two different provisions of the DMCA, Sections 512(a) and 512(c), according to Prof. Litman. Section 512(a) deals with transient material flowing through a system, while Section 512(c) deals with materials stored on a system.

Section 512(c) creates a safe harbor for companies like YouTube and SoundCloud, which store material posted by others. It provides that these hosts are not liable for such stored material, but makes this immunity subject to a notice-and-takedown regime. If a copyright owner notifies a company that some specific material being hosted is infringing, the hosting company must take down the infringing material or it will lose its safe harbor protection.

The courts have rejected past attempts to apply Section 512(c) to ISPs. "When peer-to-peer [file-sharing] began, content owners tried to use this provision to go after ISPs, but that didn't work because the alleged infringing material didn't reside on the ISPs' systems," said Litman.

ISPs (and other entities that provide internet connections) are covered by a different safe harbor provision. Section 512(a) provides that an ISP is not liable for any transient material flowing through its systems – provided the ISP did not put the material onto the system. This safe harbor protects an ISP from secondary liability arising from a customer's using the internet to upload and download infringing content. And this provision, unlike Section 512(c), does not impose a notice-and-takedown regime.

The plaintiffs in this case are trying to change that, by asserting that Section 512(i) imposes a notice-and-takedown requirement for the Section 512(a) safe harbor. If an ISP receives notice that a customer is a repeat infringer, the ISP won't take down any stored material, but instead must take down the customer's internet connection.

The record labels here "suggest failure to follow the steps prescribed by 512(c) for material residing on your servers makes an ISP liable for contributory and vicarious copyright infringement," said Litman. They are basically asserting that "Section 512(c)'s notice and takedown provision applies to Section 512(a)," she said.

This interpretation of Section 512(a) is rather dubious, according to Litman. The plaintiffs "are unlikely to prevail legally," she said.

Congress, after all, explicitly imposed a notice-and-takedown requirement for Section 512(c), while omitting that requirement for Section 512(a). And there are strong policy reasons for this distinction. It is a relatively simple matter to remove material stored on one's servers. It is far more difficult to police transient materials flowing though internet connections.

"Congress decided it would be impractical for ISPs to monitor the electronic bits that are passing through their systems," said Litman. "The University of Michigan, for example, can't possibly review all the bits of information passing through the system it supposedly controls."

Winning without Winning

If the record labels were to win this lawsuit, it could significantly strengthen the music industry's efforts to stem online infringement. Music companies could act swiftly and cheaply against tens of thousands of alleged infringers, while having ISPs perform the dirty work of cutting people off from the internet. Public ire might focus on the ISPs, not the music industry which, behind the scenes, would be forcing the ISPs to act.

However, the record labels may not really seek (or expect) to win this lawsuit. They may be using it merely as leverage, to force Cox and other ISPs to implement a more serious six-strikes policy. "This suit is really just a way to discipline Cox into passing notices of infringement to customers and terminating customers who supposedly infringe," said Sigale.

The labels filed this action "in order to scare other ISPs into a graduated response," said Litman. "This is theater more than a real lawsuit."

Perhaps, but it might just prove to be powerful and effective theater.

Image Credits: Wikimedia Commons

Related Articles:

- US Perspectives: US Tries Gentler Copyright Enforcement
- UK High Court Orders ISPs To Block Trademark-Infringing Websites
- UK Issues Tougher Draft Code For Online Copyright Infringement

Steven Seidenberg is a freelance reporter and attorney who has been covering intellectual property developments in the US for more than 15 years. He is based in the greater New York City area and may be reached at info@ip-watch.ch.