Internet Piracy 10 Years On Online Enforcement and the DMCA

By Lisa Peets and Mark Young

The Internet has done nothing less than revolutionize the way in which we share and consume music, movies, and other digital works. At the same time, it has also emerged as a highly effective vehicle for the unauthorized distribution of digital content. The Internet offers the ability to reach a global audience quickly, cheaply, and with virtual anonymity—creating the ideal opportunity for those who traffic illegitimately in the creations of others.

Recent advances in Internet technology—the vast majority of which were designed to facilitate legitimate activities—have fuelled this piracy. In the early days of the Internet, unauthorized copies of copyrighted material were offered on bulletin boards and newsgroups but usually were delivered to the end user by mail because the limited bandwidth of dial-up connections made it slow and burdensome to download relatively large digital files. Although certain newsgroups and private networks remain popular with a small minority of dedicated pirates, the increased rollout and take-up of broadband and the advent of ever more efficient file-sharing technologies today enable even relatively nontechnical users to access and download pirated digital files with ease.

Relatively early examples of "peer-to-peer" (or P2P) file-sharing technologies such as Napster and Kazaa are well-known and have been the subject of litigation around the world. More recently, BitTorrent has taken these P2P technologies one stage further. BitTorrent originally was aimed at users in search of an inexpensive way to swap open source software online. The technology makes more efficient use of bandwidth and network resources by providing for the simultaneous downloading and uploading of files. Due to its efficiency, in the past four years, BitTorrent has emerged as one of the most widely used protocols to distribute unauthorized copies of content. It now plays a key role in the piracy of business and entertainment software, audiovisual content, and books—piracy that was estimated to cause $18 billion in trade losses around the world last year (see the International Intellectual Property Alliance's Special 301 Letter to the U.S. Trade Representative dated February 11, 2008). Numerous dedicated forums, blogs, and sites that index torrent files and aggregate links to locations where files of specific types can be downloaded have sprung up to facilitate this piracy.

The Digital Millennium Copyright Act

Adopted in 1998, the Digital Millennium Copyright Act (DMCA) sought to provide a range of solutions for tackling the then-emerging problem of digital piracy. The Act includes a series of safe harbors that substantially limit the infringement liability of those online intermediaries that play a key but essentially passive role in the transmission, reproduction, and storage of illegal files online. These safe harbors do not alter the underlying analysis of whether copyright is infringed; instead, they limit the available remedies against these intermediaries to injunctive relief.[1] In general, the safe harbour provisions are designed to obviate any requirement imposed on service providers to monitor user activities. They also provide rights owners with a swift mechanism for dealing with infringement online.

Section 512 of the DMCA affords Internet service providers (ISPs) a general immunity for transmitting, routing, or providing connections for material through their systems or networks. Similarly, ISPs are immune from liability in connection with infringing material that is transmitted or stored on their service at the direction of their users or for linking users to websites or services that contain infringing material, provided that the ISP acts "expeditiously" to remove the offending content or the links to such content when they become aware of it. The DMCA contemplates that such awareness will be prompted by notices from rights holders alleging copyright infringement; to this end, the DMCA sets out requirements for what information the notices need to include, how service providers should deal with them upon receipt, and what those users whose content is the subject of a notice can do in response. This DMCA regime has spawned the widespread practice of "notice and takedown" requests to ISPs and site operators whereby copyright owners or their representatives put service providers on notice that their services are being used for copyright infringement and concomitantly demand that that service provider take action to stop it.

DMCA-Style Regimes Worldwide

While the boundaries of the DMCA regime constantly are being tested—most recently, for example, with regard to secondary liability in the *Viacom, Inc. v. YouTube Inc.*[2] and *Perfect 10, Inc. v. Amazon.com, Inc.*[3] (*Amazon.com*) litigations—the basic tenets have been exported to jurisdictions around the world. Adopted two years after the DMCA, the European Union's E-Commerce Directive,[4] for example, governs the liability of information society service providers in Europe. Like the DMCA, the E-Commerce Directive aims to strike a balance between the interests of service providers and of rights holders by means of specific activity-based immunities (focusing on "mere conduits," "caching," and "hosting"). Unlike the corresponding "safe harbors" in the DMCA, however, the E-Commerce Directive immunities relate not only to liability for copyright infringement, but to all types of liability, including tortious and criminal liability. As a result, there now exists a body of case law across EU Member States that relates to e-commerce immunities in the area of copyright, other intellectual property infringement, and defamation. Another difference from the DMCA is that the Directive does not prescribe specific rules regarding takedown

 Published in Landslide, Volume 1, Number 4, March/April 2009.

notices; consequently, the DMCA's parameters for such letters have effectively become the norm in Europe.

The U.S. government's push to incorporate DMCA-style copyright provisions and activity-specific safe harbors for service providers in free trade agreements (FTAs) with countries around the world, including Australia,[5] Bahrain,[6] Chile,[7] and Singapore[8] means that the DMCA notice and takedown regime is becoming a global norm.

Still Fit for Purpose?

Ten years on, the provisions of the DMCA that govern the liability of online intermediaries and that created the "cease and desist" online procedure continue to provide an effective tool in the fight against digital piracy. A decade of experience in addressing these issues confirms the general view that in most instances, commercial ISPs and site operators take down sites and Web pages and remove infringing links if they receive the necessary information regarding the alleged infringement. Working on behalf of a range of clients, we have found that ISP compliance rates remain high even in jurisdictions where the framework of intellectual property laws generally is perceived to be weak.

Despite the regime's effectiveness, however, some stakeholders complain about the system. Some, for example, object that ISP compliance departments too regularly remove legitimate content that is protected by fair use and other defenses at the behest of overzealous rights holders. A recent and well-publicized example of this issue involved a mother who posted a short video of her toddler son dancing to a Prince song on YouTube. Universal Music Publishing Group (UMPG) claimed the use of the song infringed its copyright; in response, YouTube pulled the video but subsequently reposted it following a challenge by the poster. Unfortunately, the episode did not end there. The Electronic Frontier Foundation filed suit against UMPG, asking a federal court to protect the fair use and free speech rights of the mother. The result was a denial of UMPG's motion to dismiss a second amended complaint, the court having emphasized that copyright owners must consider fair use before issuing takedown notices.[9]

Content users are not alone in their criticism of the DMCA. Rights holders have also expressed concerns about the system and the fact that it puts a significant burden on them to police the Internet and identify infringing conduct even in those cases where there is extensive use of sites to infringe, meaning that rights holders have to send literally tens and sometimes hundreds of thousands of takedown notices. Particularly challenging are "rogue" sites and ISPs that refuse altogether to play by the DMCA's rules. One of the most notorious examples is the Swedish torrent index site The PirateBay. BitTorrent lacks a built-in search capacity that would enable users to easily identify what content is available; instead, users are left to their own devices to find torrent files that contain data about an available illegal copy or copies of a given copyright work and about "tracker" servers that coordinate the retrieval of such files from multiple "peer" sources. The PirateBay and similar sites help users do this by categorizing—or "indexing"—torrents according to different types of protected content (music, movies, software, books, games, etc.), and they thereby arguably facilitate illegal file-sharing. Indeed, it has been estimated that The PirateBay enables more than 40 million downloads of protected content every month.

The administrators of The PirateBay have taken full advantage of open questions regarding the liability that attaches to torrent index sites, and they host the site on an ISP that refuses to comply with takedown notices. Indeed, they appear to take pleasure in flouting intellectual property protections by routinely publishing and ridiculing complaints from rights holders on their site. Not surprisingly, given its popularity with users and its refusal to respect copyright, the site is currently subject to criminal and civil proceedings in Sweden that are supported by a range of rights holders, including the motion picture and movie industries. The outcome will be closely watched both by rights holders whose works are made available on the site and by BitTorrent index site operators who have established similar business models.

Other Current Issues

Alongside the question of how to handle service providers that refuse to comply with the notice and takedown regime is the question of the potential liability of those services that do comply—and, more specifically, whether compliance with takedown notices should suffice to immunize a site operator from damages in all cases. In *Viacom, Inc. v. YouTube, Inc.*,[10] for example, now pending in the Southern District of New York, Viacom has claimed that YouTube is both directly liable for displaying, copying, and distributing a significant number of Viacom's copyrighted works and secondarily liable for the direct infringement of its users, and it is asking for extensive damages. At the heart of Viacom's claims is the argument that YouTube is more than a "passive Web host or email service" for users; Viacom claims YouTube is a full-service media outlet that directly infringes by aggregating, displaying, and distributing infringing video content. By presenting YouTube as an interactive media destination, Viacom is arguing that YouTube is not the type of passive website Congress intended to shield from liability via the safe harbor defense. Similar arguments regarding the fundamental nature of a website and whether it is a simple Web host that should be immune from liability were raised in a recent case before the Tribunal de Commerce in Paris.[11] In this case, eBay was found liable for the sale of counterfeit goods by those using the auction site and it was ordered to pay LVMH nearly €40 million in damages. The court did not dispute that Web hosts should have immunity from damages under the E-Commerce Directive but, rather, classified eBay's activities as falling outside the scope of that immunity.

Lisa Peets leads the technology and media group in the London office of Covington & Burling LLP. Her practice focuses on intellectual property and information technology, and embraces both legislative advocacy and IP enforcement. She can be reached at lpeets@cov.com. **Mark Young** is an associate in the technology and media group in Covington & Burling's London office. His practice focuses on intellectual property, information technology, and data protection law, and encompasses legislative advocacy, IP enforcement, regulatory compliance and transactional work. He can be reached at myoung@cov.com.

 Published in Landslide, Volume 1, Number 4, March/April 2009.

A second, related question is whether ISPs and other service providers have an obligation to do more to fight piracy than simply comply with takedown notices. In some markets, for example, it has been suggested that ISPs should be required to use "copyright filtering" technologies to prevent the sharing of unauthorized content or to terminate the access of subscribers who are identified as infringing copyright. This has been a particularly hotly fought issue in Europe over the past 12 months, starting in France in November 2007 with the signing of the "Olivennes" Agreement on ISP cooperation. The Agreement called for legislation to establish a (government-funded) warning and sanction mechanism aimed at deterring Internet piracy by requiring ISPs to test and implement filters, to send warning letters to subscribers involved in the exchange of pirated works, and ultimately to implement sanctions against repeat offenders—the so-called "three strikes" rule or "graduated response." While the French Senate is considering amendments to its copyright law to implement the Olivennes Agreement, the U.K. government has also been consulting on legislative options to address P2P file-sharing. It has stated that its preferred option involves a combination of codes of practice that are overseen by a regulator and that govern the activities of rights holders and ISPs, as well as obligations on ISPs to take action against subscribers to their networks who are identified (by rights holders) as infringing copyrights. An alternative option would require ISPs to allow the installation of filtering equipment that will block infringing content or require ISPs themselves to install filtering equipment that will block infringing content. In a recent press release, the U.K. government revealed that responses to the consultation indicate that there is no across-the-board support for the government's preferred co-regulatory proposal, which has caused speculation that legislation now is increasingly unlikely.

In France and the UK, and indeed across Europe, concerns have been raised regarding the effectiveness of copyright filters and the implications for user privacy; the European Parliament recently weighed in opposing these developments. It also remains to be seen how such schemes will sit alongside existing notice and takedown regimes. Ultimately, these developments and others like them serve to indicate that the battle against piracy online continues apace, both in legislatures and courts around the world, as industries continue to adapt to the Internet environment. ■

Endnotes

1. *See* Costar Group Inc. v. Loopnet, Inc., 373 F.3d 544, 552-55 (4th Cir. 2004).
2. No. 1:07-cv-02103 (S.D.N.Y. Apr. 18, 2008).
3. 508 F.3d 1146 (9th Cir. 2007).
4. 2000/31/EC.
5. *See* FTA Article 17:11(29).
6. *See* FTA Article 14:10(29).
7. S*ee* FTA Article 17:11(23).
8. *See* FTA Article 16:9(22).
9. Stephanie Lenz v. Universal Music Group Corp., Universal Music Publishing, Inc., and Universal Music Publishing Group, No. C 07-3783, Second Amended Complaint (N.D. Cal. Apr. 18, 2008).
10. No. 1:07-cv-02103 (S.D.N.Y. Apr. 18, 2008).
11. TC Paris, 1ère Ch B, June 30, 2008.

