

## INTELLECTUAL PROPERTY LITIGATION

## Expert Analysis

# Developments Reflect Growth And Confusion in Internet Practices

**O**n Jan. 12, the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet's primary governing body, will begin accepting applications for new generic top-level domains (gTLD). The gTLD program will expand permissible web address suffixes far beyond familiar extensions such as .com and .org, and will allow applications for control of virtually any domain. Any public or private organization may apply—for an initial application fee of \$185,000. A top-level domain operator would operate as the registrar for addresses using that extension. Many corporations likely will apply for domains associated with their brands or industries, meaning that the future of the Internet may feature addresses ending in .apple or .cars.

### Trademark Concerns

Opening generic top-level domains to applicants expands opportunities for cyber-squatting—bad-faith registration of a domain name confusingly similar to another party's trademark. At congressional hearings in December, opponents of the gTLD program argued that a massive increase in available domain names will make protecting trademarks from cyber-squatting much more burdensome.

LEWIS R. CLAYTON is a litigation partner at Paul, Weiss, Rifkind, Wharton & Garrison LLP and co-chair of the firm's intellectual property litigation group. He can be reached at lclayton@paulweiss.com. MATTHEW L. CONRAD, an associate with the firm, assisted in the preparation of this article.

By  
**Lewis R.  
Clayton**



They complained that organizations will have to monitor a good deal of new territory on the Internet for infringement, and may feel the need to purchase preemptively numerous domains to keep them out of the hands of cyber-squatters. Additionally, disputes may arise over who is entitled to administer a top-level domain when multiple parties attempt to lay claim.

The gTLD program will expand permissible web address suffixes far beyond familiar extensions such as .com and .org

Opposition to the gTLD program has been vigorous and diverse. The Association of National Advertisers has been a leading critic of the program and organizations from the United Nations to the International Monetary Fund have expressed concerns that their online identities would be threatened by the new domains. A Dec. 28 letter from Senator Jay Rockefeller, chair of the Senate Committee on Commerce, Science, and Transportation, asked the Department of Commerce (which oversees the contract with ICANN) to demand a delay in

implementation of the program. Nevertheless, ICANN intends to move forward as scheduled on Jan. 12.

### Protection Initiatives

ICANN has committed to fight fraud by conducting background checks of all applicants and by requiring that corporations would have priority on domains related to their trademarks, with a dispute resolution framework to address conflicts. A "rapid suspension system" would be put in place allowing challenges to allegedly infringing addresses, for a fee.

Under that system, a complainant would have to show that the registrant has no legitimate right to the name and that it is being used in bad faith. A properly made out claim would immediately freeze the name and give the registrant 14 days to respond. Within three to five days, the "system provider" will make a decision, and if warranted, transfer the domain name to the complainant. Abusive complaints may result in a temporary or permanent ban from using the complaint system.

### Lessons From .xxx

Some of the concerns trademark holders have expressed about gTLD have come to fruition in the context of another recent ICANN initiative: the April 2011 opening of the new .xxx top-level domain, intended for websites featuring adult content. Several adult websites have sued ICANN and the .xxx registry (ICM). Plaintiffs in the case, *Manwin*

*Licensing International v. ICM Registry*, filed in Los Angeles federal court on Nov. 16, claim that both ICANN's creation of the new top-level domain and the process by which defendant ICM obtained registry rights violated the antitrust laws and forced trademark holders to make numerous and expensive defensive registrations.

In December, Google purchased youtube.xxx in what is perceived as a move to prevent potential cyber-squatters from using that domain to damage its brand. Owners of other well-known marks may take similar preemptive action as hundreds or thousands of new domains are introduced. Apparently anticipating litigation, ICANN is reportedly earmarking a significant percentage of each \$185,000 gTLD application fee for legal costs.

Time will tell whether the fears of ICANN's critics come to pass. Though the potential harm is not yet imminent—the first new top-level domains will likely not go live until as late as 2013—the new year may be one of uncertainty for trademark holders worldwide.

### Trademark

*Ascentive, LLC v. Opinion Corp.*, 2011 WL 6181452 (E.D.N.Y. Dec. 13, 2011), reinforces the limits of trademark law's power against "gripe sites" and demonstrates how allegedly unethical use of trademarks is not coextensive with infringing use. Plaintiffs, marketers of anti-virus software and mattresses, were the subject of negative user reviews on Opinion Corp.'s website, "PissedConsumer.com." The website operated by providing a forum for consumers to publish criticisms about businesses on sub-domains such as "ascentive.pissedconsumer.com"—then allegedly offering expensive "reputation management services" to the target businesses that would allow responses, de-emphasis, or even removal of negative reviews.

Among other claims, plaintiffs alleged that Opinion Corp. violated the Lanham Act by using their marks in domain names, on review pages and through techniques that plaintiffs claimed were designed to result in higher search

engine placement. In particular, plaintiffs claimed that Opinion Corp. engaged in illicit Search Engine Optimization (SEO) techniques, such as republishing years-old reviews through Twitter to improve the review's Google results, leading to initial interest confusion.

In denying a preliminary injunction, the court in the Eastern District of New York held that initial interest confusion does not occur when a consumer clicks on a search result that criticizes the mark used in the user's search. And the court suggested that the remedy for unethical SEO tactics lies not under the Lanham Act, but through raising the issue with the manipulated search engine. The opinion concluded by noting that while Opinion Corp.'s practices were troubling, no trademark remedy was available.

---

The Northern District of California in '*Fraley v. Facebook*' rejected Facebook's argument that it was immunized from liability by the Communications Decency Act, holding that Facebook is a content provider outside the scope of CDA immunity.

*Fraley v. Facebook Inc.*, 2011 WL 6303898 (N.D. Cal. Dec. 16, 2011), addresses publicity rights in the social networking context. The case arises from Facebook's January 2011 introduction of "Sponsored Stories," automated Facebook postings that inform a user's connections that the user endorses a Facebook advertiser when the user clicks the "Like" button on the advertiser's page. Plaintiffs, users whose names were used on Sponsored Stories, alleged that this constituted commercial misappropriation of their names and likenesses under several California statutes.

The Northern District of California noted that similar challenges to Facebook's advertising techniques had been dismissed in the past because plaintiffs could not show they were injured financially by the misappropriation of their likenesses in commercial endorsements. Here, however, the court was convinced by Facebook's own marketing, which

claims that the commercial recommendation of a friend is worth significantly more than that of a stranger. By pointing to this specific example of the value of consumer endorsements to marketers, plaintiffs were able to allege the existence of economic damages and gain Article III standing to challenge use of their likenesses.

The court also rejected Facebook's argument that it was immunized from liability by the Communications Decency Act (CDA), holding that Facebook is a content provider outside the scope of CDA immunity. More than just rearranging text provided by users, Facebook reworked "Likes" into advertisements, allegedly transforming their character and vitiating Facebook's protection under the CDA.

### Copyright

*Elsevier Ltd. v. Chitika Inc.*, 2011 WL 6008975 (D. Mass. Dec. 2, 2011), illustrates the difficulty of establishing a contributory infringement claim given the nature of advertising on the Internet. Plaintiffs brought infringement claims against a resident of India who was making their copyrighted material available for free download. Plaintiffs also alleged contributory infringement by Chitika, a service that provides advertisements to websites in exchange for a share of the advertising proceeds. Plaintiffs alleged that by arranging advertising for the website, Chitika profited from the infringement and enabled the website to remain in business.

Dismissing the claim, the Massachusetts district court held that the plaintiffs failed to allege that Chitika possessed the requisite knowledge of the infringing activity to be liable for contributory infringement. The court explained that "Plaintiffs do not allege facts showing that Chitika was familiar with the content" of the infringing website, or "knew (or had reason to know) that such content was infringing." The court also noted that websites that contract with Chitika represent that they do not have any infringing content and agree not to display the ads on pages with infringing

material. The court further found that Chitika did not materially contribute to any infringement because there were no satisfactory allegations that revenue derived from the ads assisted the allegedly infringing activities.

*UMG Recordings Inc. v. Shelter Capital Partners LLC*, 2011 WL 6357788 (9th Cir. Dec. 20, 2011), held that mere general knowledge that an Internet service could be used to share unauthorized copies of copyrighted material is insufficient to strip the service provider of immunity under §512 of the Digital Millennium Copyright Act (DMCA). Defendant Veoh Networks Inc. operates a website that allows users to upload and share videos. UMG Recordings alleged that by allowing the posting of videos containing their copyrighted musical works, Veoh violated UMG's rights under the DMCA.

Veoh claimed immunity under §512 of the DMCA, which provides a safe harbor only if the service provider did not have actual knowledge that the material is infringing. UMG argued that this requirement was not satisfied because, given the nature of Veoh's service and the knowledge that it could be used to host infringing material, it must have known there was unauthorized content.

The U.S. Court of Appeals for the Ninth Circuit rejected UMG's interpretation of the knowledge standard, holding that under this theory, the DMCA would be "rendered a dead letter." The court noted that UMG decided to forgo the usual DMCA protocol under which claimants give notice of infringement to the provider, leaving them without evidence that Veoh had actual notice that they were hosting infringing material. The unanimous panel explained that requiring specific knowledge serves the law's policy goals because copyright holders are in a better position to identify infringing copies than providers like Veoh for whom, given the volume of material they host, it would be a "practical impossibility" to ensure that no infringing material is ever uploaded.

Two district court cases highlight the difficulty associated with enforcing copyright against anonymous parties.

First, *Maximized Living Inc. v. Google Inc.*, 2011 WL 6749017 (N.D. Cal. Dec. 22, 2011), clarifies the reach of a copyright owner's subpoena power under §512 of the DMCA.

A John Doe republished Maximized Living's copyrighted material on a blog hosted by Google. Maximized Living applied for a subpoena under §512(h), demanding from Google documents revealing the alleged infringer's identity. Doe moved to quash the subpoena, arguing that he had removed the copyrighted material by the time the subpoena was requested, and that the DMCA only authorizes subpoenas regarding currently infringing material, not past infringement.

The magistrate judge ordered that the subpoena be quashed. A §512 subpoena requires notification to the service provider of the material "that is to be removed or access to which is to be disabled," which Doe argued cannot be given when the material has already been taken down. The court agreed with this reading, and was also influenced by the argument that the subpoena power is closely tied to the DMCA's notice-and-takedown provisions, which cannot be applied when the material has already been removed. Thus, the court concluded, the subpoena power does not reach past infringing activity. Any remedies for past infringement no longer subject to a takedown notice would have to be created by Congress.

Second, *People Pictures, LLC v. Group of Participants in Filesharing Swarm*, 2011 WL 6758462 (D.D.C. Dec. 23, 2011), demonstrates jurisdictional challenges that can arise in mass copyright litigation. Plaintiff owned the copyright for a film that was allegedly distributed without authorization over the Internet. The plaintiff asked for pre-conference discovery in the form of subpoenas to service providers to determine the identities associated with the IP addresses associated with the distribution. The magistrate judge refused to authorize the subpoenas on the ground that Federal Rule of Civil Procedure 26(f) requires "good cause" to engage in "jurisdictional" discovery. Plaintiff failed to show, how-

ever, that the users of the IP addresses in question would be within the court's jurisdictional reach under the District of Columbia long-arm statute, or that the district court would be the proper venue for claims against those users under the Copyright Act.

## Patents

Over the past three years, the U.S. Court of Appeals for the Federal Circuit has on several occasions issued extraordinary writs of mandamus, directing district courts to transfer patent infringement cases to more convenient forums. A number of those decisions concerned the Eastern District of Texas, which has become a major focus of patent litigation, in part because of its liberal approach to venue.

In *In re Link\_A\_Media Devices Corp.*, 662 F.3d 1221 (Fed. Cir. 2011), the Federal Circuit issued a writ to direct transfer of a patent case from Delaware to the Northern District of California, despite the fact that the defendant was a corporation incorporated under Delaware law. Other than defendant's incorporation there, Delaware had "no ties to the dispute or to either party." Plaintiff was a holding company incorporated in Bermuda, whose operating subsidiary was based in northern California, only three miles from the defendant's headquarters. The Court of Appeals also rejected plaintiff's argument that Delaware federal judges are "highly experienced in patent infringement litigation." The Northern District of California was "equally equipped" to address patent claims.