Moving Upstream With a Large Paddle

By: Lawrence G. Walters & Kevin W. Wimberly

Walters Law Group

www.FirstAmendment.com

The adult industry often finds itself at the center of precedent-setting legal battles. Some of these cases have clarified or even changed the law. For example, the *Hustler* cases created precedent in the defamation and copyright fields; *Victor's Little Secret* brought about the Trademark Dilution Revision Act; the *Perfect 10* cases have defined the contours of DMCA safe harbor protection; and *Playboy* has established First Amendment principles in attempts to regulate decency in telecommunications.[1]

Recently, the adult industry has been making increased appearances in mainstream technology & law media such as TechDirt, ars technica, and the Electronic Frontier Foundation ("EFF") website.[2] In fact, as reported by XBIZ, the EFF was recently appointed to represent various Doe defendants in one of the many bittorrent/Doe copyright infringement cases brought by adult content producers.[3] While the "massive Doe" litigation strategy is beyond the scope of this article, one cannot help but note that this strategy is receiving much the same criticism that the RIAA MP3-sharing strategy received near the turn of the century.[4] (The strategy was recently analyzed by respected adult Internet attorney Greg

---

[1] *Hustler Magazine, Inc. v. Falwell,* 485 U.S. 46 (1988); *Moseley v. V Secret Catalogue, Inc.*, 537 U.S. 418 (2003); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007); *Perfect 10, Inc. v. CCBILL LLC*, 488 F. 3d 1102 (9th Cir. 2007); *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803 (2000).

[2] Nate Anderson, "Judge eviscerates P2P lawyer: 'I accepted you at your word,'" *Ars Technica,* n.d. Available at: http://arstechnica.com/tech-policy/news/2011/03/judge-eviscerates-p2p-lawyer-i-accepted-you-at-your-word.ars; Mike Masnick, "More Mass Porn Copyright Infringement Lawsuits Get Dumped," *TechDirt.com,* January 3, 2011. Available at: http://www.techdirt.com/articles/20110101/21182712478/more-mass-porn-copyright-infringement-lawsuits-get-dumped.shtml; Mike Masnick, "Unicorns And Leprechauns Aren't Real... But Trolls Are (And They Have Lawyers)," *TechDirt.com,* March 11, 2011. Available at: http://www.techdirt.com/articles/20110311/12332513464/unicorns-leprechauns-arent-real-trolls-are-they-have-lawyers.shtml; "Copyright Trolls," *Electronic Frontier Foundation,* n.d. Available at: http://www.eff.org/issues/copyright-trolls.

[3] See http://www.xbiz.com/news/news_piece.php?id=130171.

[4] Grant Gross, "Congress Scrutinizes RIAA Tactics," *PCWorld,* September 17, 2003. Available at: http://www.pcworld.com/article/112535/congress_scrutinizes_riaa_tactics.html; John Schwartz, "She Says She's No Music Pirate. No Snoop Fan, Either." *The New York Times,* September 25, 2003. Available at: http://www.nytimes.com/2003/09/25/business/media/25TUNE.html?ex=1098849600&en=6960e362c873ed2e&ei=5070; "Not-so-Jolly Rogers," *Economist.com Global Agenda,* September 10, 2003. Available at: http://www.economist.com/agenda/PrinterFriendly.cfm?Story_ID=2050467.

Piccionelli, Esq., in "*Bittorrent Legal Mania.*")[5] In addition to its lack of effectiveness, the recording industry abandoned that strategy after receiving backlash from traditional media publications, such as *Rolling Stone*, and by legal scholars, who were concerned by the lack of due process and extortion-like qualities that make up certain flavors of the mass-Doe model.[6]

Regardless of one's opinion of the mass-Doe strategy, one thing is generally accepted by all sides: Those who infringe copyrights (or other intellectual property rights) must be held accountable.

However, punishing infringers is not the only piece of the equation. To a certain extent, the adult industry has become overly-dependent on traditional DVD and full-length film distribution, charging hefty retail purchase prices, or imposing recurring monthly billing in exchange for access to extensive libraries of content. To some extent, the customer's tastes and expectations changed, but many content producers failed to follow suit. Thus, in addition to pursuing infringers, adult producers need to develop some form of content-protection technology, and – like the music industry - recognize the consumer's desire for micropayments and a per-song vs. a per-album business model. One can only wonder whether the industry would be experiencing the same level of rampant piracy of its content, if end users were provided the opportunity to pay a reasonable fee for the specific content they want, as opposed to the prevailing monthly billing model. At least one company has envisioned the future, and reacted, as evidenced by Pink Visual's new PVLocker.com platform, the release of which has recently been hailed by XBIZ as "redefining" content distribution.[7] Admittedly, even if such distribution and protection mechanisms are developed and implemented, there will still be infringement on the Internet. There will always be people unwilling to pay for content for whatever reason. But, as many reformed Napster.com music file infringers now use iTunes at 99 cents a pop, those companies turning to micropayments for specified clips may see the same kind of results.

The Problem

Internet-based infringement typically occurs in one of two ways: (1) distributed infringement via bittorrent; and, (2) client/server infringement via cyberlockers or other Web-based locations. Each has legal and technological hurdles that copyright owners must overcome in order to bring infringers to justice – or at least make them pay up.

Infringement via bittorrent

Bittorrent is a technology that gained popularity as the "-ster" (Napster, Aimster, Grokster) peer-to-peer applications were either judicially shut down or were otherwise forced to "go legit" in the

---

[5] See http://www.xbiz.com/articles/legal/131701.

[6] Sarah McBride and Ethan Smith, "Music Industry to Abandon Mass Suits," *The Wall Street Journal*, December 19, 2009. Available at: http://online.wsj.com/article/SB122966038836021137.html?mod=rss_whats_news_technology.

[7] See http://www.xbiz.com/news/news_piece.php?id=130211.

face of being shut down. From a functionality perspective, rather than a user connecting to another user's computer to download an entire file (as in the "-ster" P2P apps), bittorrent drastically increases the efficiency and speed of downloads by allowing a downloader to receive "pieces" of a file from multiple other users who either possess the entire file or pieces of it.[8] In the time it used to take to download a single MP3, for example, bittorrent allows an entire album to be downloaded. From a legal perspective, this provides a massive list of potential unauthorized distributors and downloaders.

The torrent infringement model lends itself to massive amounts of anonymous defendants based on the basic architecture of the bittorrent protocol. While this is somewhat of an oversimplification, there are no real culpable intermediaries in the bittorrent protocol. Other than a bittorrent user's Internet service provider (Comcast, Bellsouth, Roadrunner, etc.), there are essentially no upstream intermediaries to contact, such as a discussion forum and/or cyberlocker's actual host. (An example of a cyberlocker is *Rapidshare*.) While bittorrent does rely on a "tracker" server to initiate communication among downloaders, the tracker server does not need to contain any copyrightable material to operate, and the tracker is not necessary after the downloaders, or "peers," have been "introduced." As a result, there are no gatekeepers capable of removing actual content or otherwise available to receive other legal methods attempting to stop the conduct – the only persons or entities possessing the infringing content are the downloaders. The content owner seeking to stop infringement via bittorent thus has limited options – try to shut down the tracker server, which will just reappear under a new name and at a new location, or sue the individual sharers and stealers of the content and rely on deterrence of future user-based infringement. [9]

Bittorrent software clients enable the user (and others) to see the Internet Protocol addresses ("IP address") of the machines providing and downloading the pieces of the files, and it is those IP addresses that presumably match up with the Does in the mass-Doe lawsuits.

As recent procedural hurdles have shown, however, courts are reluctant to allow plaintiffs to lump hundreds of Does into the same lawsuit when such Does may reside in multiple jurisdictions and have unique defenses (such as "My wireless network isn't secure; a virus took over my machine; it must have been my neighbor…").[10]

However difficult it may be to litigate against multiple bittorrent users at once, these plaintiffs, many of which are adult content producers, are generally seeking out the appropriate targets – those who are infringing copyrights with knowledge of doing so. Nobody can reasonably dispute that those

---

[8] "What is BitTorrent?" *Bittorrent.com.* Available at: http://www.bittorrent.com/btusers/what-is-bittorrent.

[9] John Borland, "Feds shut down BitTorrent hub," *Cnet News,* May 25, 2005. Available at: http://news.cnet.com/Feds-shut-down-BitTorrent-hub/2100-1028_3-5720541.html; Michael Ingram, "LokiTorrent caves to MPAA," *Slyck.com*, February 10, 2005. Available at: http://www.slyck.com/news.php?story=661

[10] Lawrence G. Walters, "Beggars Can't Be Forum Choosers," *Xbiz.com*, March 22, 2011. Available at: http://www.xbiz.com/blogs/larrywalters.

who make the conscious efforts and decisions to either rip, share, and/or download content without authorization should be held legally accountable.

What *is* subject to legitimate debate among e-commerce scholars and attorneys is how far the law does and should go when determining intermediary liability for infringement based on more traditional server/client models.[11] Such intermediaries include discussion forums, cyberlockers, tube sites, and even hosts or billing processors.

Infringement via discussion forums and cyberlockers

The typical example of this type of infringement is as follows: Someone sets up a discussion forum that allows users to register and post links or other content on the forum. Users often upload content to a cyberlocker and then post the link to the file (which is hosted by the cyberlocker) on the discussion forum. Presuming that the file is a video, the user may also post a screenshot, thumbnail, or description of the video file on the discussion forum. Other users of the forum can then click the link to the cyberlocker and begin downloading the file. Some forums even allow users to upload content to the forum itself, thereby eliminating the need for a cyberlocker. This is typically the case when the content being illegally distributed is limited to still images or text.

At first glance, the traditional client/server model therefore provides plaintiffs with easily-identifiable targets that don't exist in the bittorrent model. For the sake of argument, potential defendants include the user who posted the content or links to the cyberlocker, the cyberlocker itself, the cyberlocker's host, the operator of the discussion forum, and the discussion forum's host. Upon researching the status of these people and entities, however, it is often the case that the discussion forum operator is based overseas, has provided misinformation in the WHOIS database when registering its domain, provides no contact information on the site, and/or is generally unreachable absent great expense. The same goes for the user that uploaded the content or provided the links to the cyberlocker. The user is often identified only by a nickname, and without cooperation from the forum operator it is therefore difficult if not impossible, to uncover the user's IP address. All the content owner wants to do is send a DMCA Notice, but there is no readily available recipient.

At this point, plaintiffs start looking upstream. If they cannot easily find the direct infringers and those who really induced the infringement, then why not send DMCA Notices to the people hosting the forum and/or cyberlocker? These hosts are often based in the United States and provide hosting services to thousands of other customers unrelated to the infringing activity. They are easy targets and often have deep pockets. By moving upstream, the content owner is typically focused on two interests – removal of its content and/or squeezing out settlement money.

---

[11] "Secondary and Intermediary Liability on the Internet," Stanford Technology Law Review 2011 Symposium, March 3, 2011. Information available at: http://stlr.stanford.edu/symposia/2011-secondary-liability-online/; Robert D. Atkinson, et al., "The Next Digital Decade: Essays on the Future of the Internet," *TechFreedom*, 2010. Available at: http://nextdigitaldecade.com/contents.

While the authors contend that a host providing hosting services to a website or forum that offers user-generated content should not be required to process DMCA Notices based on its customers' users' conduct and content, that very scenario is becoming commonplace. In 2009, Microsoft sent a DMCA notice to Network Solutions concerning one document found on the Cryptome website, which Network Solutions hosted.[12] Networks Solutions asked its customer to remove the file, and the customer refused, citing fair use. Since Network Solutions did not have the means to remove that single document from its customer's site, it shut down the entire site, taking with it thousands of lawful documents and speech. Similarly, in 2009 the U.S. Chamber of Commerce sent a DMCA Notice to an upstream ISP concerning a parody site hosted by the ISP. When the ISP contacted its customer about the site, the customer explained that the site was a parody. Rather than spend the time and money to stand up for its customer – or at least evaluate the defense – the ISP terminated the customer's account and thereby shut down many other websites that the customer operated in addition to the parody site.[13]

Countless other examples exist where upstream service providers are getting dragged into disputes between content owners and alleged infringers. Our firm has represented hosts and other service providers named in litigation where they had only a remote, contractual relationship with the real wrongdoer. The effect on free speech is obvious. While this may just seem like the case of a spineless ISP, such lack of spine is understandable in typical circumstances. Faced with being dragged into litigation to defend itself from a claim of secondary liability based on its customers' material, it is easier and more economical for the host to just comply with the DMCA Notice and deny continued hosting services to the entire account, even though the host is a neutral intermediary.

To the content owner, this is of no concern. The content was removed. To believers in free speech and the rule of law, the concerns are troubling.

Irrespective of one's stake in the game, the practice of holding intermediaries responsible for the actions of its customers' end users should alarm all involved. If the host (or billing company or other intermediary) has DMCA safe harbor protection – or even if it does not have DMCA safe harbor but could still successfully mount a "no secondary liability" defense – then why wouldn't it assert those protections and defenses to allow the online communications to continue? The answer is simple: economics. For a host, the cost of defending itself in a secondary liability infringement case in federal court is almost guaranteed to exceed the hosting fees that the customer pays. While the DMCA allows the end user to serve a "counter-notification," the intermediary's direct customer (i.e. the actual site hosting the content) may not have actual knowledge of the facts relating to the infringement sufficient

---

[12] Corynne McSherry, "The Weakest Link Redux," *Electronic Frontier Foundation,* March 4, 2010. Available at: http://www.eff.org/deeplinks/2010/03/weakest-link-redux.

[13] "Chamber of Commerce Takes Aim at Yes Men: Business Group Tries to Take Down Parody Site After Embarrassing Prank," *Electronic Frontier Foundation,* October 22, 2009. Available at: http://www.eff.org/press/archives/2009/10/22.

to allow it to serve a counter with the required certification under the penalties of perjury.[14] Moreover, by serving several DMCA notices on an intermediary, relating to customers' end users' activity, the specter of "repeat infringer" rears its head. The intermediary may need to terminate the customer, who may operate a plethora of sites unrelated to the infringing content - even if counter-notifications are served to some of the DMCA infringement notifications – depending on the Repeat Infringer Policy adopted by the host. However, by terminating the customer's account or otherwise not giving the customer the opportunity to dispute the alleged infringement, the host saves enormous amounts of time and money dealing with notices, counter-notifications, and related communications. Many of these communications need to be reviewed by legal counsel, thus increasing the cost of compliance and maintaining the customer's account.

Once terminated, the customer is forced to find a new host, and it may seek hosting services overseas in the hopes to avoid future DMCA-related terminations. This would ultimately frustrate any future infringement pursuits by content owners. Also, by imposing increasing monitoring and compliance obligations on hosts, the costs of hosting naturally increases, and the hosts pass along the mounting legal costs, operational costs and insurance premiums to their customers. As more hosts are dragged into costly litigation for the misdeeds of their customers – or even their customers' customers – there is less incentive to provide the services to begin with. Regrettably, this is a textbook example of the chilling effect on speech. This also creates an incentive for an underground (or overseas) market for hosting risky user-generated content. Not surprisingly, these hosts simply ignore DMCA obligations, and can therefore provide the services at a lower cost. Content owners may therefore end up in a much worse position by blindly naming domestic intermediaries as defendants, as opposed to working with these companies in a cooperative fashion.

Conclusion

The mass-Doe litigation model is still in its infancy. Some plaintiffs are having success, and some are failing in a very public manner. It is too early to tell what effect these cases will have on the law or the rules of procedure that govern the law. Regardless of that outcome or the ultimate strategy used in these bittorrent cases, it is wise to consider the ultimate practical and economic impact on these intermediary service providers prior to giving in to the temptation to name the "deep pocket" in litigation. Ease of identification and financial wherewithal should not be the primary motivating factors for naming a defendant. What may seem like a quick and easy payoff has lasting First Amendment and economic effects that will reverberate long after content is removed (and undoubtedly replaced the next day by a different user, on a different forum, with a different host.) This is a time of opportunity for content owners. New piracy protection measures, micro-payment systems, personalized content "locker" distribution– all of these can be implemented as realistic responses to the torrents of infringement. But, seeking to impose liability on easy targets with remote involvement in any infringing activity threatens to impose crushing financial burdens on an already ailing industry while also pushing the law in a direction that threatens the true expression of ideas in the online marketplace.

---

[14] *See*, 17 U.S.C. § 512(g)(2)&(3).

Lawrence G. Walters, Esq., heads up ***Walters Law Group****, a law firm which represents clients involved in all facets of the adult industry. Kevin Wimberly, Esq., is an associate with the firm, and concentrates on intellectual property matters and new media law. The firm handles First Amendment cases nationwide, and has been involved in Free Speech litigation at all levels, including the United States Supreme Court. All statements made in the above article are intended for general informational purposes only and should not be considered legal advice. Please consult your own attorney on specific legal matters. You can reach Lawrence Walters at* larry@firstamendment.com *or Kevin Wimberly at* kevin@firstamendment.com*. More information about* ***Walters Law Group*** *can be found at* www.FirstAmendment.com*.*