ARTICLE:

ELECTRONIC EVIDENCE IN TORRENT COPYRIGHT CASES

By **Thomas M. Dunlap** and **Nicholas A. Kurtz**

Introduction

This article explores the methodology behind obtaining electronic evidence of peer-to-peer users and the use of that evidence in current copyright infringement actions in United States Federal Courts. Over the last year and a half, a number of lawsuits have been filed on behalf of film copyright holders seeking to enforce their rights against users of peer-to-peer (P2P) torrent-type technologies used to unlawfully download and distribute films.

At the time of filing their complaints, the plaintiffs have only been able to identify the Doe defendants by their internet Protocol (IP) address, the file hash, file title, and the date and time of the alleged infringement. The only way that the plaintiffs can determine the defendants' actual names is by obtaining the information from the internet Service Providers (ISPs) to which the defendants subscribe and from which the defendants obtain internet access, as this information is readily available to the ISPs from documents and data they keep in the regular course of business.

Part II of this article will explore the basic methodology behind the investigation of torrent users that infringe the plaintiffs' copyrights. Part III will explore the process of obtaining court orders to subpoena the ISPs for the defendants' identifying information. Finally, Part IV will explore the identification and subpoena production process of the various ISPs.

The investigation and identification of IP addresses infringing copyrights

Basic U.S. copyright law

The Copyright Act provides that the owner of a copyright has the exclusive rights to reproduce and to distribute copies of the registered copyrighted work.[1] The Copyright Act further provides that anyone who violates any of the exclusive rights of the copyright owner is an infringer of the copyright.[2]

Pursuant to the Copyright Act, a plaintiff may elect to recover statutory damages instead of actual damages or the infringer's profits. 17 U.S.C. § 504(c) provides: "the copyright owner may elect, at any time before final judgment is rendered, to recover, instead of actual damages and profits, an award of statutory damages for all infringements involved in the action, with respect to any one work ... in a sum of not less than $750 or more than $30,000 as the court considers just." Section 504(c) further provides that where an infringement is committed willfully, a court has the discretion to increase the award of statutory damages to $150,000.[3]

Pursuant to the Copyright Act, a plaintiff may also recover its costs and attorneys' fees. 17 U.S.C. § 505 provides: "[i]n any civil action under this title, the court in its discretion may allow the recovery of full costs by or against any party other than the United States or an officer thereof. Except as otherwise provided by this title, the court may also award a reasonable attorney's fee to the prevailing party as part of the costs."

As alleged in the plaintiffs' complaints in the various P2P piracy cases, the Doe defendants, without authorization, used an on-line media distribution system to download the plaintiffs' copyrighted motion pictures and distributed them to other users on the P2P network.

Overview of the P2P infringing activity

The internet is a vast collection of interconnected computers and computer networks that communicate with each other. It allows hundreds of millions of

1 17 U.S.C. § 506(1), (3).
2 17 U.S.C. § 501(a).
3 17 U.S.C. § 504(c)(2).

people around the world to freely and easily exchange ideas and information, including academic research, literary works, financial data, music, audiovisual works, graphics, and an unending and ever-changing array of other data. Unfortunately, the internet also has afforded opportunities for the wide-scale infringement of copyrighted motion pictures. Once a motion picture has been transformed into an unsecured digital format, it can be copied further and rapidly distributed an unlimited number of times over the internet at little or no cost to the distributor, without significant degradation in picture or sound quality.

To copy and distribute copyrighted motion pictures over the internet, many individuals use on-line media distribution systems or commonly called P2P networks. P2P networks, at least in their most common form, are computer systems that enable internet users to (1) make files (including motion pictures) stored on each user's computer available for copying by other users; (2) search for files stored on other users' computers; and (3) transfer exact copies of files from one computer to another via the internet.

At any given moment and depending on the particular P2P network involved, anywhere from thousands to millions of people, either across the country or around the world, unlawfully use the P2P network to connect to one another's computers to upload (distribute) or download (copy) copyrighted material. The P2P systems represent a "viral" distribution of digital files: each user of the system who copies a digital file from another user can then distribute the file to other users and so on, so that copies of an infringing file can be distributed to millions of people worldwide at breathtaking speed.

Further, a person who uses a P2P network is free to use any alias (or "network name") whatsoever, without revealing his or her true identity to other users. Thus, while a copyright holder may have observed infringement occurring on the internet, it cannot know the true identities of those individuals who are committing the infringement on a P2P network.

Additionally, these torrent P2P methodologies make even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file provider intentionally elects to share a file using a P2P network. This is called "seeding." Other users (peers) on the network connect to the seeder to download. As additional peers request the same file, each additional user becomes a part of the network (or "swarm") from where the file can be downloaded. However, unlike a traditional peer-to-peer network, each new file downloader is receiving a different piece of the data from each user who has already downloaded that piece of data, all of which pieced together comprise the whole. This means that every "node" or peer user who has a copy of the infringing copyrighted material on a P2P network – or even a portion of a copy – can also be a source of download for that infringing file, potentially both copying and distributing the infringing work simultaneously.

This distributed nature of P2P leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a P2P protocol, every seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a possible source for the subsequent peer, providing any one of those seed peers is on-line at the time the subsequent peer downloads a file.

Additionally, it has been shown that the use of the torrent platform is primarily for the infringement of copyrights. As noted in a January 2010 study by a Princeton University Senior Sauhard Sahi,[4] approximately 99 per cent of all files on BitTorrent were infringing copyrights (10 of the 1021 files were found to be likely non-infringing), with 100 per cent of movie and television files found to be infringed content. A study from the University of Ballarat in Australia found that no legal samples of either movies, music or television shows in their sample of 1,000 torrents on the BitTorrent network:

> Through our investigations, we found that 43.3% of BitTorrent torrents are movies, 29.1% are TV shows and 16.5% are music. Using our sample of trackers we discovered that a total of 117 million current seeds are available across more than one million torrents, based on the number of seeders available for the files. The top two files were being seeded more than one million times each and the third

4 *Under the supervision of Princeton Professor Ed Felten; a summary is available at https://freedom-to-tinker.com/blog/felten/census-files-available-bittorrent; for a more recent study that supports the work of professor Felten and Sauhard Sahi, see 'Technical report: An Estimate of Infringing Use of the Internet' (January 2011, Version 1.8, Envisional Ltd, Cambridge, UK), available at http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf.*

> more than 500,000 times. In summary, our results indicate that 89% of all torrents from our sample are confirmed to be infringing copyright, both by the number of files and total number of current seeders. Of the torrents in the top three categories (Movies, Music and TV shows), there were no legal torrents in the sample.[5]

A more recent study in January of 2011 found that approximately 23.8% of all global internet traffic is infringing on copyrighted content with BitTorrent specifically accounting for almost half of that amount, supporting both the Princeton and Ballarat studies.[6]

Preliminary identification of defendants

Plaintiffs in P2P piracy cases utilize the services of various technology companies to monitor their films. These companies engage in a specific process utilizing specially designed software technology to identify direct infringers of the plaintiffs' copyrights using protocols investigated by the companies' software on P2P networks. All of the infringers named as Doe defendants were identified by the companies' software connecting to files of illegal versions of the plaintiffs' motion pictures. All infringers connected to those files are investigated through downloading a part of the file placed on their computer. The companies then save this evidence.

Once the companies' searching software program identifies an infringer, the companies obtain the IP address of a user offering the file for download. When available, the companies also obtain the user's pseudonym or network name and examine the user's publicly available directory on his or her computer for other files that lexically match the motion picture. In addition to the file of the motion picture itself, the companies download or otherwise collect publicly available information about the network user that is designed to help the plaintiffs identify the infringer. Among other things, the companies download or record for each file downloaded: (a) the time and date at which the file or a part of the file was distributed by the user; (b) the IP address assigned to each user at the time of infringement; and, in some cases, (c) the video file's metadata (digital data about the file), such as title and file size, that is not part of the actual video content, but that is attached to or contained within the digital file and helps identify the content of the file. The companies then create evidence logs for each user that store all this information in a database.

An IP address is, in combination with the date, a unique numerical identifier that is automatically assigned to a user by its ISP each time a user logs on to or obtains access to the network. Each time a subscriber logs on, he or she may be assigned a different (or "dynamic") IP address unless the user obtains from his/her ISP a static IP address. ISPs are assigned certain blocks or ranges of IP addresses by the Internet Assigned Numbers Authority (IANA) or a regional internet registry such as the American Registry for Internet Numbers (ARIN). ISPs keep track of the IP addresses assigned to their subscribers at any given moment and retain such "user logs" for a very limited amount of time, sometimes as little as weeks or even days, before erasing the data they contain. These user logs provide the most accurate – and often the only – means to connect an infringer's identity to its infringing activity.

Although users' IP addresses are not automatically displayed on the P2P networks, any user's IP address is readily identifiable from the packets of publicly available data being exchanged. The exact manner in which the companies determine a user's IP address varies by P2P network.

An infringer's IP address is significant because it is becomes a unique identifier that, along with the date and time of infringement, specifically identifies a particular computer using the internet. However, the IP address does not enable the companies to ascertain with certainty the exact physical location of the computer or to determine the infringer's identity. It only enables the companies to trace the infringer's access to the internet to a particular ISP.

Publicly available databases located on the internet list the IP address ranges assigned to various ISPs. However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. Because these ISPs consequently have no direct relationship – customer, contractual, or otherwise – with the end-user, they are not able to identify the Doe defendants through reference to their user logs, but they can identify the intermediary ISP

5 Robert Layton and Paul Walters, 'Investigation into the content of infringing content of BitTorrent network' (April 2010, Internet Commerce Security Laboratory, University of Ballarat, Australia), available at http://www.afact.org.au/research/bt_report_final.pdf.

6 See 'Technical report: An Estimate of Infringing Use of the Internet- Summary' (January 2011, Version 1.8, Envisional Ltd, Cambridge, UK), available at http://www.mpaa.org/Resources/8aaaecf5-961e-4eda-8c21-9f4f53e08f19.pdf.

to which that IP address has been allocated.

The technology companies then download the motion picture file, or a substantial part of it, and the other identifying information described above, and creates evidence logs for each Doe defendant. Once the companies identify the ISP used by the Doe defendants to gain access to the internet from the IP address, an e-mail is sent to the relevant contact at each ISP informing them of the Doe defendant's IP address and the date and time of the infringing activity. The message requests that each ISP retain the records necessary to identify the subscriber who was assigned that IP address at that date and time. Once provided with the IP address, plus the date and time of the infringing activity, the Doe defendant's ISPs quickly and easily can use their respective subscriber logs to identify the name and address of the ISP subscriber who was assigned that IP address at that date and time.

Finally, the companies confirm that the digital audiovisual files it downloaded are actual copies of the relevant motion picture. It is possible for digital files to be mislabeled or corrupted, therefore the companies (and accordingly, the plaintiffs) do not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the motion picture themselves.

Typically, a member of the companies watches a DVD copy of the motion picture provided by plaintiff. After the companies identify the Doe defendants and downloaded the motion pictures they were distributing, the companies open the downloaded files, watch them, and confirm that they contain a substantial portion of the motion picture.

Obtaining authorization to conduct discovery to identify the Doe defendants

After the plaintiffs file their complaints, typically listing the IP addresses that the plaintiffs have discovered and ensuring that they correspond to infringement of the plaintiffs' copyrights, the plaintiffs must then conduct discovery on the ISPs to obtain the personal identifying information for each IP address.

Fed. R. Civ. P. Rule 26(d)(1) prohibits a party from "seek[ing] discovery from any source before the parties have conferred as required by Rule 26(f), except in a proceeding exempted from initial disclosure under Rule 26(a)(1)(B), or when authorized by these rules, by stipulation, or by court order." However, courts routinely allow discovery to identify "Doe" defendants.[7]

In similar copyright infringement cases brought by motion picture studios and record companies against Doe defendants, the courts have consistently granted the plaintiffs' motions for leave to take expedited discovery to serve subpoenas on ISPs to obtain the identities of Doe defendants prior to a Rule 26 conference.[8]

Overall, courts have wide discretion in discovery matters and have also allowed expedited discovery when "good cause" is shown.[9]

Doe defendant challenges to expedited discovery

Defendants in P2P downloading cases have sought to dismiss the complaint or to protect their private information from disclosure by bringing one of three defenses:

7 *For instance, Murphy v. Goord, 445 F.Supp.2d 261, 266 (W.D.N.Y. 2006) (in situations where the identity of alleged defendants may not be known prior to the filing of a complaint, the plaintiff should have an opportunity to pursue discovery to identify the unknown defendants); Wakefield v. Thompson, 177 F.3d 1160, 1163 (9th Cir. 1999) (error to dismiss unnamed defendants given possibility that identity could be ascertained through discovery); Valentin v. Dinkins, 121 F.3d 72, 75-76 (2d Cir. 1997) (plaintiff should have been permitted to conduct discovery to reveal identity of defendant); Dean v. Barber, 951 F.2d 1210, 1215 (11th Cir. 1992) (error to deny plaintiff's motion to join John Doe defendant where identity of John Doe could have been determined through discovery); Munz v. Parr, 758 F.2d 1254, 1257 (8th Cir. 1985) (error to dismiss claim merely because defendant was unnamed; "Rather than dismissing the claim, the court should have ordered disclosure of Officer Doe's identity"); Gillespie v. Civiletti, 629 F.2d 637, 642 (9th Cir. 1980) ("where the identity of alleged defendants [are not] known prior to the filing of a complaint . . . the plaintiff should be given an opportunity through discovery to identify the unknown defendants"); Maclin v. Paulson, 627 F.2d 83, 87 (7th Cir. 1980) (where "party is ignorant of defendants' true identity . . . plaintiff should have been permitted to obtain their identity through limited discovery"); Equidyne Corp. v. Does 1-21, 279 F. Supp. 2d 481, 483 (D. Del. 2003) (allowing pre-Rule 26 conference discovery from ISPs to obtain identities of users anonymously posting messages on message boards).*

8 *See Warner Bros. Records, Inc. v. Does 1-6, 527 F.Supp.2d 1, 2 (D.D.C. 2007) (allowing plaintiffs to serve a Rule 45 subpoena upon Georgetown University to obtain the true identity of each Doe defendant, including each defendant's true name, current and permanent addresses and telephone numbers, e-mail address, and Media Access Control (MAC) address) (citing Memorandum Opinion and Order, UMG Recordings, Inc. v. Does 1-199, No. 04-093(CKK) (D.D.C. March 10, 2004); Order, UMG Recordings v. Does 1-4, 64 Fed. R. Serv. 3d (Callaghan) 305 (N.D. Cal. March 6, 2006)).*

9 *See Warner Bros. Records, Inc. v. Does 1-6, 527 F.Supp.2d 1, 2 (D.D.C. 2007); Semitool, Inc. v. Tokyo Electron Am., Inc., 208 F.R.D. 273, 275-76 (N.D. Cal. 2002); Qwest Comm. Int' l, Inc. v. WorldQuest Networks, Inc., 213 F.R.D. 418, 419 (D. Colo. 2003); Entm' t Tech. Corp. v. Walt Disney Imagineering, No. Civ. A. 03-3546, 2003 WL 22519440, at *4 (E.D. Pa. Oct. 2, 2003) (applying a reasonableness standard: "a district court should decide a motion for expedited discovery on the entirety of the record to date and the reasonableness of the request in light of all of the surrounding circumstances") (quotations omitted); Yokohama Tire Corp. v. Dealers Tire Supply, Inc., 202 F.R.D. 612, 613-14 (D. Ariz. 2001) (applying a good cause standard).*

1. Under FED R. CIV P. 20(a)(2) that they have been improperly joined as the defendants are allegedly engaging in "separate but similar behavior by individuals allegedly using the internet to commit copyright infringement";[10] and

2. That the plaintiffs lack the requisite personal jurisdiction to require an out of state defendant to be hauled into a Federal Court where such defendant does not reside and as such their identifying information should not be released to the plaintiffs; and

3. That the defendants have the right to engage in anonymous communication via torrent platforms under the First Amendment's guarantee of free speech.

Permissive joinder

The Federal Rules of Civil Procedure allow defendants to be permissively joined in one action when claims arise from the same transaction or occurrence or series of transactions or occurrences; and any question of law or fact in the action is common to all defendants.[11] Further the court must consider whether joinder would prejudice any party.

With respect to the first requirement, in *Maverick Entertainment, Call of the Wild Movie* and *Donkeyball Movie*, the Federal Court considered the plaintiffs' allegations of the actions of individual P2P infringers on a torrent network, as well as the nature of a true P2P network, where each downloader is also an uploader and vice versa.[12] The court found that the individual P2P infringers were necessarily logically related enough to satisfy this requirement at this early stage in the civil process, as a result of the defendants' use of a file sharing protocol in multiple jurisdictions and their use of multiple computers to illegally distribute the plaintiffs' films.[13]

Further in the same cases, the court found common questions of law, and found that the plaintiff in each instance would have to establish the same set of facts as to any defendant concerning the validity of the underlying copyright, the existence of infringement, and use of the same torrent file-sharing protocol to illegally distribute and download the plaintiffs' motion pictures. The court concluded that, "consequently, factual issues related to how BitTorrent works and the methods used by plaintiffs to investigate, uncover and collect evidence about the infringing activity will be essentially identical for each putative defendant."[14]

With respect to the issue of prejudice to any party, the court found that judicial economy would not be served by severing the defendants as a remedy for improper joinder, as the plaintiffs would be "forced to file 5,583 separate lawsuits, in which they would then move to issue separate subpoenas to ISPs for each defendant's identifying information. Plaintiffs would additionally be forced to pay the Court separate filing fees in each of these cases, which would further limit their ability to protect their legal rights. This would certainly not be in the interests of convenience and judicial economy, or secure a just, speedy, and inexpensive determination of the action."[15]

Personal jurisdiction defense

To obtain personal jurisdiction over a defendant, a plaintiff must satisfy both the requirements of due process and of the jurisdictional long arm statute of the forum state, which is sometimes more restrictive and sometimes coterminous with the requirements of due process. Due process requires that a defendant have "minimum contacts" with a forum such that "the defendant's conduct and connection with the forum State are such that he should reasonably anticipate being haled into court there."[16] Plaintiffs faced with a motion to dismiss an action are entitled to reasonable discovery on the moving defendant's contacts with the forum state. As the discovery phase of litigation is the only matter at issue before the court in P2P Doe cases, the only requirement is that a plaintiff allege that a putative defendant have some possible connection with the forum.[17]

The First Amendment and free speech

Finally, amici and some Doe defendants in torrent P2P

10 *Judge B. Howell, quoting Amici American Civil Liberties Union in Call of the Wild Movie, LLC v. Does 1–1,062, 2011 WL 1807416 (D.D.C. 2011).*
11 *Fed. R. Civ. P. 20(a)(2); see also Montgomery v. STG Int'l, Inc., 532 F. Supp. 2d 29, 35 (D.D.C. Jan. 30, 2008) (interpreting Rule 20(a)(1), which has the same requirements as Rule 20(a)(2)).*
12 *Call of the Wild Movie, LLC v. Does 1–1,062, 2011 WL 1807416 (D.D.C. 2011).*
13 *Call of the Wild Movie, LLC v. Does 1–1,062, 2011 WL 1807416 (D.D.C. 2011).*
14 *Call of the Wild Movie, LLC v. Does 1–1,062, 2011 WL 1807416 (D.D.C. 2011) at 10.*
15 *Call of the Wild Movie, LLC v. Does 1–1,062, 2011 WL 1807416 (D.D.C. 2011) at 12 internal quotations omitted.*
16 *World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980).*
17 *Humane Soc'y of the United States v. Amazon.com, Inc., No. 07-623, 2007 U.S. Dist. LEXIS 31810, at *10 (D.D.C. May 1, 2007); Virgin Records Am., Inc. v. Does 1-35, No. 05-1918, 2006 WL 1028956, at *3 (D.D.C. Apr. 18, 2006).*

downloading cases have attempted, unsuccessfully, to allege a basis for First Amendment protection raising the question as to whether the putative defendants are engaging in any expressive communication when they share files through P2P networks that would entitle them to some protection of their anonymity under the First Amendment of the U.S. Constitution. In *London-Sire Records, Inc. v. Doe 1*,[18] the court found that some creative aspects of downloading or making P2P content available were potentially expressive such that the speech could be worthy of some level of protection:

a) the value judgment of what is worthy of being copied;

b) the association of one recording with another by placing them together in the same library;

c) the self-expressive act of identification with a particular recording;

d) the affirmation of joining others listening to the same recording or expressing the same idea.

However, the "aspect of a file-sharer's act that is infringing is not entitled to First Amendment protection, other aspects of it are."[19]

In *Call of the Wild*, Amici Electronic Frontier Foundation provided an affidavit stating "BitTorrent provides users with less ability to identify and communicate with the peers with whom they exchange files than other technologies do … There is no easy way for the various BitTorrent users who have uploaded or downloaded parts of a file to recognize, name, or communicate with one another."[20] This affidavit was submitted in support of the proposition that the defendants are not properly joined; however the court in that case found this supported the notion that speech on torrent P2P networks is worthy of even less First Amendment protection than other types of file sharing networks.[21]

Courts in the United States have generally applied the five part test described in *Sony Music Entertainment v. Does 1-40*,[22] to determine the level of First Amendment protection that should be awarded to anonymous internet activities. The more restrictive test formulated in the defamation case of *Dendrite International v. Doe*[23] has generally not been adopted in file-sharing cases.[24] The *Sony* test balances five factors to assess if the plaintiffs' need for identifying information outweighs the defendants' right to First Amendment anonymity. The issues of concern are:

(1) the concreteness of the plaintiffs' showing of a *prima facie* claim of actionable harm;

(2) the specificity of the plaintiffs' discovery request;

(3) alternative means to get the information the plaintiffs seek;

(4) the need for the information to advance the plaintiffs' claim; and

(5) the objecting party's expectation of privacy.

The primary issue in these cases is usually the defendants' expectations of privacy. Courts in the United States have universally found that defendants do not have an expectation of privacy, in part by virtue of their subscriber agreements with their ISP, in which the defendants freely disclose their personal information to a third party, and which agreements generally put the defendants on notice that the ISP may be monitoring for infringement and may disclose information to third parties. For example, Time Warner Cable's subscriber agreement states:

> Time Warner Cable's subscribers and account holders may not upload, post, transmit or otherwise make available on or via the Road Runner Service any material protected by copyright in a manner that infringes that copyright. In accord with the Digital Millennium Copyright Act, it is the policy of Time Warner Cable to terminate in appropriate circumstances the Road Runner Service of any subscriber or account holder who is a repeat

18 *London-Sire Records, Inc. v. Doe 1,542 F. Supp. 2d 153, 161 n.7 (D. Mass. 2008).*

19 *London-Sire Records, Inc. v. Doe 1,542 F. Supp. 2d 153, 161 n.7 (D. Mass. 2008) at 163. See also Sony Music Entm't, Inc. v. Does 1-40, 326 F. Supp. 2d 556, 568 (S.D.N.Y. 2004) and Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 555-57, 560 (1985) (finding copyright infringement is not protected by the First Amendment).*

20 *Amici Reply Brief, Seth Schoen Decl. in Support of Reply Brief ¶9, Call of the Wild.*

21 *See also Arista Records LLC v. Does 1-19, 551 F. Supp. 2d 1, 8 (D.D.C. 2008) (finding that a file sharer's First Amendment right to anonymity is exceedingly small.)*

22 *Sony Music Entertainment v. Does 1-40, 326 F. Supp. 2d at 564-65.*

23 *Dendrite International v. Doe, 775 A.2d 756.*

24 *For instance, see London-Sire, 542 F. Supp. 2d at 164 n.2.*

> infringer. . . . Time Warner Cable expressly reserves the right to terminate or suspend the service of any subscriber or account holder even for a single act of infringement.[25]

Courts have repeatedly, and without variance on this subject, found that a putative defendant's asserted First Amendment right to anonymity in context of P2P file sharing does not create any shield from allegations of copyright infringement.

In summary, in applying for expedited discovery, plaintiffs in P2P piracy cases have consistently been granted orders to conduct discovery and subpoena the ISPs for the Doe defendants' personal identifying information. Courts have routinely found that the plaintiffs established good cause for the discovery because: (1) the plaintiffs have sufficiently identified the Doe defendants through the unique IP address each Doe defendant was assigned at the time of the unauthorized distribution of the copyrighted motion pictures, (2) the plaintiffs specifically identified the steps taken to identify defendants' true identities, (3) the plaintiffs asserted a prima facie claim for direct copyright infringement in their complaints, (4) the plaintiffs' claims for copyright infringement presumes irreparable harm to the copyright owners that is worsened by the fact that ISPs typically retain user activity logs containing the information sought for only a limited period of time before erasing the data, and (5) the plaintiffs' need for the information greatly outweighs any privacy or First Amendment interest the Doe defendants have in such speech.[26]

The ISPs' ability to identify the Doe defendants and comply with subpoenas

Because of the way data is maintained by the various ISPs, each ISP has a particular process by which it associates an IP address with one of its subscribers. Because most consumer IP addresses are "dynamic," compared to "static," most ISPs engage in multiple processes in order to respond to a subpoena.[27] Static IP addresses are addresses that remain set for a specific user indefinitely, while dynamic IP an ISP randomly assigns addresses to its subscriber and change frequently. Associating a dynamic IP address with a particular customer on a specific day and time makes the task of "discovering the identity of a particular infringer more difficult."[28] This requires ISPs to maintain logs and other records, and to use commercially available or customized software tools, to correlate the IP address assigned to a computer at a specific moment with the subscriber's account information in order to identify a customer from the IP address, either for the ISPs own internal business purposes or to respond to subpoenas requesting identifying information about a customer.[29]

While most ISPs are able to respond to these subpoenas as requested, or work out arrangements with the counsel of the plaintiffs, some ISPs have sought to quash or limit the subpoenas. In particular, Time Warner Cable has argued that it cannot respond to subpoenas in P2P cases because its resources are already fully utilized in responding to law enforcement requests.[30]

However, in *Maverick Entertainment, Call of the Wild Movie* and *Donkeyball Movie*, the Federal court found that "Time Warner has failed to demonstrate that compliance with the plaintiffs' subpoena requests would impose an undue burden."[31] In giving little weight to Time Warner's conclusory affidavits, the Federal court noted that other ISPs were able to produce identifying information for hundreds of IP addresses per month.[32] Ultimately, "Court sees no reason why Time Warner cannot expeditiously complete the processing of this information for production to the plaintiffs."[33]

Additionally, the amici have repeatedly argued that the Doe defendants must be notified that their identifying information is being sought before the ISPs respond to the subpoena. Further, because many of the ISPs also provide cable television to their subscribers, the ISPs believe they are bound to notify

25 *http://www.timewarnercable.com/nynj/about/policies/regulatorynotices/subscriberagreement/.*
26 *See Maverick Entertainment Group, Inc. v. Does 1–2,115, 2011 WL 1807428 (D.D.C. 2011), Voltage Pictures, LLC v. Does 1–5,000, 2011 WL 1807438 (D.D.C. 2011), Call of the Wild Movie, LLC v. Does 1–1, 062, 2011 WL 1807416 (D.D.C. 2011), Donkeyball Movie, LLC v. Does 1–171, 2011 WL 1807452 (D.D.C. 2011), followed in MCGIP, LLC v. Does 1-18, 2011 WL 2181620 (N.D. Cal. 2011).*
27 *See generally London–Sire, 542 F.Supp.2d at 160.*
28 *London–Sire, 542 F.Supp.2d at 160; see also U.S. v. Steiger, 318 F.3d 1039, 1042 (11th Cir. 2003) ("Static addresses are undoubtedly easier to trace, but ISPs generally log the assignments of their dynamic addresses.").*
29 *For instance, see Klimas v. Comcast Cable Commc' n, Inc., 465 F.3d 271, 275 (6th Cir. 2006) ("dynamic IP addresses constantly change and unless an IP address is correlated to some other information, such as Comcast's log of IP addresses assigned to its subscribers ..., it does not identify any single subscriber by itself.") Internal quotations omitted.*
30 *See Call of the Wild Movie, LLC v. Does 1-1,062, --- F.Supp.2d ----, 2011 WL 996786 at *17 (D.D.C. March 22, 2011).*
31 *Call of the Wild Movie, LLC v. Does 1-1,062, --- F.Supp.2d ----, 2011 WL 996786 at *20 (D.D.C. March 22, 2011).*
32 *Call of the Wild Movie, LLC v. Does 1-1,062, at *18.*
33 *Call of the Wild Movie, LLC v. Does 1-1,062, at *20.*

their subscribers pursuant to the Cable Act. Therefore, many court orders allowing plaintiffs to conduct discovery require the ISPs to notify their subscribers that their identifying information is being sought, and these orders give the Doe defendants time to file a motion with the courts.

Conclusion

To enforce their copyrights against P2P piracy, the rights holders and their attorneys must engage in a substantial process just to identify the infringers. This process starts with the investigation and gathering of electronic data at the torrent sites, to identify IP addresses associated with infringement of the plaintiffs' works. This data is then used to subpoena identifying information from various ISPs, each of which use their own systems to process the data. Ultimately, the plaintiffs are able to obtain the identity of the individuals associated with the infringement of the plaintiffs' works and enforce their rights against individual downloaders of content. To date there have been a number of Doe suits in the United States where the court has entered judgment against the individual infringer on a torrent platform.[34]

Thomas M. Dunlap is the co-founder and partner of Dunlap, Grubb & Weaver and was named one of the "100 Most Powerful Lawyers 2010" by the Hollywood Reporter. Tom currently serves as faculty for Virginia CLE's Intellectual Property Seminar and has spoken on IP litigation and copyright all over the world.

Nicholas A. Kurtz is an associate at Dunlap, Grubb & Weaver, where he practices copyright and entertainment litigation. Nicholas has handled litigation cases involving films such as Cars 2 (with Tom Dunlap), Spiderman and The Tooth Fairy (starring Dwayne "the Rock" Johnson).

http://www.dglegal.com/

tdunlap@dglegal.com

34 *West Bay One v. Libic, (EDVA, Richmond Division, Case No. 3:11-cv-00057-REP, Doc. 12 & 13, July, 2011). Achte/Neunte Boll Kino Beteiligungs Gmbh & Co KG v. Plebaniak, (D. Mass., Eastern Division, Case No. 11-10268-PBS, Docs. 13, 14 & 15.)*

