New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 247—NO. 38
TUESDAY, FEBRUARY 28, 2012

Expert Analysis

SOUTHERN DISTRICT CIVIL PRACTICE ROUNDUP

# Protecting Copyright Holders And Potential Infringers

By **Edward M. Spiro**

And **Judith L. Mogul**

As use of the Internet grows, so too does the prevalence of cyber torts and related litigation. One of the biggest challenges facing potential plaintiffs in these cases often lies in identifying who the defendants are and where they are located. These determinations present distinct if not unique procedural wrinkles and have become something of a proving ground for new approaches to classic problems. In this fast-developing area, where courts and litigants are educating themselves and becoming increasingly sophisticated, new issues evolve as others are resolved. A pair of recent decisions from the U.S. District Court for the Southern District of New York, both involving efforts by copyright holders to identify infringers known only by their Internet Protocol (IP) addresses, illustrate the competing interests at stake and some of the outcome-influencing factors in these cases.

Southern District Judge Paul A. Crotty's decision in *Digiprotect USA Corp. v. Does 1-240*,[1] and Southern District Judge Alison J. Nathan's decision in *Digital Sin Inc. v. Does 1-176*,[2] each concerned efforts by copyright holders of different "adult" films to pursue infringement claims against individuals who had allegedly used a software called BitTorrent to download and distribute unauthorized copies of the films in question through peer-to-peer networks.

BitTorrent allows groups of interacting users known as a "swarm" to download, share and aggregate small bits of extremely large files so that they may efficiently view a film that might otherwise take several days to download in its entirety. Individuals who participate in a "swarm" expose their IP addresses while downloading and sharing a file, enabling the copyright holder to determine the IP address but no other identifying information concerning the infringer. In each of the two cases discussed below, the plaintiff copyright holders commenced actions against multiple John/Jane Doe defendants associated with the infringing IP addresses, and then sought expedited discovery from the Internet Service Providers (ISPs) aimed at discovering the identity of the subscriber associated with the offending IP address.

## Personal Jurisdiction

Judge Crotty granted the plaintiff's order to show cause directed at the ISPs in *Digiprotect*, subject to the ISPs' rights to challenge the order. In fact, two of the ISPs served with subpoenas seeking subscriber information, Time Warner and Comcast, sought to modify the order based on the burden and expense of compliance. At a subsequent conference, Judge Crotty, apparently sua sponte, raised the issue of personal jurisdiction, vacating the subpoena and dismissing the complaint with leave to replead only as to those Doe defendants over whom there was prima facie jurisdiction by virtue of defendant-specific connection to New York.

> In two cases, plaintiff copyright holders sought expedited discovery from the ISPs aimed at discovering the identity of the subscriber associated with the offending IP address.

In rejecting plaintiff's personal jurisdiction arguments, Judge Crotty drew heavily from an earlier decision by Southern District Judge Thomas P. Griesa in an almost identical case brought by the same plaintiff concerning a different motion picture.[3] Judge Crotty found that the New York State Court of Appeals' decision in *Penguin Group (USA) Inc. v. American Buddha*,[4] locating in New York the situs of injury when a New York copyright holder's rights are infringed on the Internet, was not dispositive. First, he questioned whether that rule would extend to the plaintiff in this case, that held highly limited rights to distribute the copyrighted work over peer-to-peer networks, while most of the bundle of rights associated with the work in question remained with an out-of-state company.

But even assuming alleged injury in New York, Judge Crotty found, as Judge Griesa had before him, that the plaintiff in this case had not made the additional required showing under New York's long-arm statute permitting the exercise of jurisdiction over a defendant who commits a tortious act outside the state. Specifically, plaintiff had not shown that any of the Doe defendants would reasonably have expected their actions in downloading this film to have consequences in New York or that the unnamed defendants derived substantial revenues from interstate or international commerce.[5]

Judge Crotty went on to reject the plaintiff's argument that the fact that peer-to-peer networks connect out-of-state defendants with in-state defendants is sufficient to confer personal jurisdiction over all defendants. Noting that plaintiff had not alleged that the defendants were conspiring together or acting as each others' agents, he found that just because BitTorrent users may have downloaded the same motion picture did not mean that they were part of the same "swarm" and that there was thus no evidence that the defendants acted together.

He concluded that the plaintiff could only proceed against defendants subject to jurisdiction in New York if, for example, they reside in New York or illegally downloaded the movie while physically present in the state. He dismissed the case with leave to replead only as to that group of defendants.

Again citing Judge Griesa's earlier ruling, Judge Crotty expressed concern about "'ensnar[ing] unsophisticated individuals from around the country in a lawsuit based in New York,' who likely would be encouraged to settle rather than incur the burden and embarrassment of contesting the

EDWARD M. SPIRO *and* JUDITH L. MOGUL *are principals of Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer, both concentrating in commercial litigation. Mr. Spiro is co-author of "Civil Practice in the Southern District of New York," 2d Ed. (Thomson West 2011).*

litigation."[6] Judge Crotty was, however, as much concerned with the burden this type of litigation imposes on the third-party ISP providers as with the burden on potential defendants. He required the plaintiff to determine which defendants were sufficiently connected to New York for jurisdictional purposes (something that can be done through publicly available sources that match IP addresses with geographic regions), rejecting the plaintiff's request that the ISPs be ordered to supply this information. He also granted a protective order limiting the number of IP address look-ups a month an ISP could be required to undertake, and requiring plaintiff to reimburse the ISPs for the costs of each look-up and required subscriber notification.

### 'Digital Sin'

The plaintiff in *Digital Sin v. John Does 1-176* heeded the lessons of *Digiprotect*, performing pre-suit reverse-IP checks on the suspect IP addresses and filing an action naming only those defendants whose IP addresses indicated they were likely located in New York. Although the plaintiff passed this threshold jurisdictional hurdle, Judge Nathan subjected its initial ex parte application for expedited discovery to rigorous scrutiny on three other grounds, expressing serious concerns regarding privacy, joinder and potential misidentification of defendants, in addition to the ex parte, expedited nature of the discovery request.

### Ex Parte Expedited Discovery

As a threshold matter, Judge Nathan assessed whether the plaintiff had made the requisite showing of good cause for expedited discovery, noting that "particularly careful scrutiny" of such requests is in order where the request is ex parte.[7] She accepted the plaintiff's assertion that ISPs routinely erase the type of account information sought, and observed that those ISPs qualifying as cable operators could not supply subscriber information without a court order,[8] in concluding that no reasonable alternative would enable the plaintiff to identify or serve the defendants so that the litigation could proceed.

### Robust Protective Order

Although Judge Nathan concluded that some "cabined" expedited discovery was appropriate, she authorized that discovery only after plaintiff agreed to a robust protective order designed to protect the ISP subscribers whose identities were sought. She articulated a concern that the subscribers identified might not be the individuals who had actually downloaded the copyrighted "adult" material in question, noting that the plaintiff's counsel had acknowledged as much as a 30 percent mismatch between subscriber and downloader. (Plaintiff's "counsel stated that the true offender is often the 'teenaged son…or the boyfriend if it's a lady'" and the Court noted that the perpetrator could also be a neighbor in an apartment building or dormitory that has a shared network or IP address).

Citing accounts of harassment by copyright holders who had obtained court-ordered subscriber information from ISPs, Judge Nathan crafted a protective order designed to reduce the risk that false positives might result in "'coerc[ed] unjust settlements from innocent defendants such as individuals who want to avoid the embarrassment of having their names publicly associated with allegations of illegally downloading 'My Little Panties #2.'"[9] Specifically, with plaintiff's consent, she took the unusual step of permitting defendants to proceed anonymously.[10]

The protective order also set out detailed timing requirements permitting identified subscribers ample time to challenge the subpoena: She ordered that (1) the ISPs have 60 days from service of the subpoena seeking subscriber information to serve the subscribers with a copy of the subpoena and the protective order; (2) the subscribers have 60 days from service by the ISPs of the subpoena and order to contest the subpoena (through a motion to quash or modify) as well as to request to litigate anonymously; (3) any subscriber who makes such a motion or request inform its ISP so that it does not release the information as to that subscriber's identity; and (4) the ISPs have 10 days following the expiration of the second 60-day period to produce the subpoenaed information for any Doe defendant who has not made a motion or request.[11]

Although Judge Nathan concluded that some 'cabined' expedited discovery was appropriate, she authorized that discovery only after plaintiff agreed to a robust protective order designed to protect the ISP subscribers whose identities were sought.

### Joinder Concerns

Judge Nathan also considered whether the 176 Doe defendants were properly joined in the action before her under Federal Rule of Civil Procedure 20(a)(2), which permits joinder of multiple defendants where the plaintiff's claims for relief arise out of the same transaction, occurrence or series of transactions and occurrences. She noted that cases involving "swarm" infringement cases have come out both ways—with some finding misjoinder of large groups of defendants and others finding joinder proper in similar circumstances.[12] Ultimately, she accepted the plaintiff's argument that it had carefully selected only a small group of New York defendants who traded the same, identifiable file as part of the same "swarm" during a relatively short six-week window.

Acknowledging that at least one court had found a similar pattern of usage to be an insufficient basis for joinder, she concluded that "it is difficult to see how the sharing and downloading activity alleged in the Complaint—a series of individuals connecting either directly with each other or as part of a chain or 'swarm' of connectivity designed to illegally copy and share the exact same copyrighted file—could not constitute 'a series of transactions or occurrences' for purposes of Rule 20(a)."[13] Although she declined to sever the case at that early discovery stage, Judge Nathan noted that she would revisit the question if the Doe defendants came forward with conflicting defenses.

### Conclusion

Resourceful uses of technology that facilitate infringement as well as its detection also lead to clashes of rights and interests belonging to copyright holders, potential defendants and third-party ISPs. Potential defendants are often absent at the critical early stages of these litigations, and are often constrained by resources and reputational risk from mounting a vigorous, meaningful defense to infringement charges once they are identified. Courts have taken an active role in protecting these ISP subscribers as they balance the competing procedural and substantive interests at stake.

1. 2011 WL 4444666 (S.D.N.Y. Sept. 26, 2011) ("*Digiprotect II*").
2. 2012 WL 263491 (S.D.N.Y. Jan. 30, 2012).
3. *Digiprotect USA Corp. v. Does 1-266*, 2011 WL 1466073 (S.D.N.Y. April 13, 2011) ("*Digiprotect I*").
4. 16 N.Y.3d 295, 921 N.Y.S.2d 171 (2011).
5. 2011 WL 4444666, at *2 (citing *Digiprotect I*, 2011 WL 1466073, at *4 and N.Y. C.P.L.R. §302(a)(3)).
6. 2011 WL 4444666, at *3 (quoting *Digiprotect I*, 2011 WL 1466073, at *2).
7. 2012 WL 263491, at *2 (quoting *Ayyash v. Al-Madina*, 233 F.R.D. 325, 327 (S.D.N.Y. 2005) (Lynch, J.)).
8. 47 U.S.C §551(c) prohibits ISPs qualifying as "cable operators" from disclosing subscriber information without a court order and notice to the subscriber.
9. 2012 WL 263491 at *3 (quoting *SBO Pictures Inc. v. Does 1-3036*, 2011 WL 6002620, at *4 (N. D. Cal. Nov. 30, 2011)). Judge Nathan noted that the plaintiff's lawyer had "bluntly conceded" "horror stories" about what some law firms had done with subscriber information.
10. See, e.g., *John Wiley & Sons Inc. v. John Does Nos. 1-27*, 2012 WL 364048 (S.D.N.Y. Feb. 3, 2012) (Pauley, J.) (finding risk of potential copyright liability inadequate justification for copyright defendant's application to proceed anonymously).
11. The protective order contained other provisions, including an order to the ISPs to preserve all information pending resolution of timely filed motions to quash; instructions for ISPs seeking reimbursement of costs associated with compliance; and a directive that information obtained through the subpoenas be used solely for the purpose of protecting the plaintiff's rights as set forth in the complaint.
12. 2012 WL 263491, at *4 and nn.1 & 4-5 (citing cases).
13. 2012 WL 263491, at *5 (citing *Digiprotect II*, 2011 WL 4444666, at *3 n.3 and disagreeing with *Hard Drive Prods. Inc. v. Does 1-188*, 2011 WL 3740473, at *13 (N. D. Cal. Aug. 23, 2011)).