New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 247—NO. 61
FRIDAY, MARCH 30, 2012

Outside Counsel

Expert Analysis

Pre-Action Disclosure Of Internet Speakers' Identities

Every day innumerable people "speak" on the Internet, through e-mail, social media, blogs and other electronic writings, without disclosing their identities (or by using fictitious ones). But the anonymity of Internet speech becomes an issue when one feels aggrieved by anonymous (or pseudonymous) words. And although the First Amendment protects anonymous speech, that protection is not absolute. Increasingly, would-be plaintiffs—particularly those claiming defamation based on Internet speech—resort to the courts to unmask the electronic speaker's identity. New York's pre-action disclosure statute provides a well-suited mechanism for doing so, although using it for this purpose raises unsettled issues.

Disclosure Under §3102(c)

Section 3102(c) of CPLR authorizes disclosure "[b]efore an action is commenced…to aid in bringing an action… but only by court order." The request typically is by a special proceeding under CPLR Article 4. To obtain pre-action disclosure, the petitioner must show that (i) a meritorious cause of action exists and (ii) the information sought is material and necessary to that wrong.[1]

An accepted purpose of Section 3102(c) disclosure is to obtain the identity, where unknown, of the party responsible for the asserted wrongdoing.[2] In this sense, Section 3102(c) "offer[s] broader pre-action discovery than comparable federal procedure [under] Fed. R. Civ. P. 27(a),"[3] which authorizes only pre-action depositions to perpetuate testimony. Federal courts have therefore held that Rule 27(a) is not to be used to identify would-be defendants.[4] In federal court, an alternative—albeit perhaps more difficult—approach is to sue "Doe" defendants and seek expedited discovery under Rule 26(f) to uncover their identities from third parties.[5]

Internet's Attributes

The architecture of the Internet provides many ways for cyberspace speakers to shield their identities. A fundamental building block is the Internet Protocol (IP) address, which links every computer/user connected to the Internet. Blocks or ranges of IP addresses are assigned to Internet service providers (ISPs), like America Online and Verizon, which in turn assign the IP addresses to their subscribers. While an IP address affords a level of anonymity, knowledge of the IP address and the date/time of a communication generally enables an ISP to identify the computer from which the communication originated and often the name of the subscriber controlling the computer.

SCOTT M. HIMES *is a member of Stillman & Friedman. He focuses his practice on complex commercial litigation.*

By
Scott M. Himes

But further layering of Internet communication is common. Electronic communication through websites (related web "pages" containing certain content) is "hosted" on a web server accessible via a computer network. Innumerable and often anonymous "posts" are published daily on websites through blogs, on message boards and the like. Moreover, a party can acquire a "domain name" for a website (the well-known ".com," ".org," etc.) register the domain name through a private registration service and arrange for a separate provider to host the website. That provider, in turn, might contract through cloud services or other connectivity for the website to be hosted by another provider on its servers. In fact, various entities in this website chain promote "privacy" as a key feature of their services and are designed to offer online anonymity.

The architecture of the Internet provides many ways for cyberspace speakers to shield their identities.

Another consideration when actionable speech is published on the Internet is the federal Communications Decency Act. It creates immunity from liability for providers and users of an "interactive computer service" who publish information originating from others.[6] Unlike for traditional media, ISPs and similar entities are protected from claims based on the content published on their websites or communications on their systems, as long as they are not involved in content creation or development. This protection underscores the need to identify the "speaker" responsible for the offending Internet content.

Differing Requirements

An important early case is *Sony Music Entertainment Inc. v. Does 1-40*.[7] Although it is a Southern District decision, *Sony's* standards have been applied in Section 3102(c) proceedings. Plaintiff record companies sued "Doe" defendants for copyright infringement arising from downloading and distributing plaintiffs' music from the Internet. Plaintiffs subpoenaed a non-party ISP (Cablevision) to obtain defendants' identities, asserting that Cablevision could identify defendants from IP addresses traced to them. Cablevision's "Terms of Service" prohibited subscribers from transmitting materials in violation of copyright and other laws and gave Cablevision the right to disclose "any information as necessary to satisfy any law, regulation or other governmental request." The court ordered Cablevision to give notice of the subpoena so the affected subscribers could move to quash.

After recognizing that the First Amendment protects anonymous speech, but not absolutely, the court endorsed a balancing test for determining whether anonymous Internet speakers' identities should be disclosed. The factors are: (1) a concrete showing of a prima facie claim of actionable harm; (2) specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) a central need for the information to advance the claim; and (5) the party's expectation of privacy.

On these factors, the court declined to quash the subpoena, ruling that "defendants' First Amendment right to remain anonymous must give way to plaintiffs' right to use the judicial process to pursue what appear to be meritorious copyright infringement claims."[8]

Soon after, a New York trial court applied *Sony's* balancing test to a Section 3102(c) application in *Public Relations Society v. Road Runner High Speed Online*.[9] Petitioners sought documents from ISP Road Runner that would identify the "John Doe" who, they claimed, sent defamatory e-mail. Road Runner defaulted, but "John Doe" contested disclosure. After concluding that one of the petitioners had a meritorious defamation claim, the court held that *Sony's* factors outweighed "John Doe's" right to anonymity and authorized pre-action disclosure of his identity.

Similarly, in *Greenbaum v. Google Inc.*,[10] petitioner claimed she was defamed on a Google blog and sought pre-action disclosure of the identities of the anonymous blog operator and bloggers. Concerned that the anonymous speakers receive notice, the court directed service on the blog operator. While citing *Sony* and other cases that adopted a balancing test, the court also accepted the disclosure requirements set forth in a New Jersey appellate court decision, *Dendrite International Inc. v. Doe*.[11] That decision keyed on (i) notice to the anonymous speaker and an opportunity to be heard; (ii) specification of the particular statements alleged to be defamatory; and (iii) an "evidentiary showing" of the merits of the proposed defamation claim. On the last *Dendrite* consideration, *Greenbaum* noted that other cases applied a "lesser standard" in gauging a proposed claim's merits, using different formulations; however, *Greenbaum* did not reach the "quantum of proof" issue because the statements were deemed not actionable as defamation. The court therefore denied disclosure.

Another court within the U.S. Court of Appeals for the Second Circuit elaborated on the "merits showing" factor in *Doe I v. Individuals*.[12] Plaintiffs subpoenaed an ISP to determine who had posted website comments about them. Notice was given to the person associated with the IP address in issue, and "John Doe" appeared and moved to quash. The court endorsed a balancing analysis on the *Sony* and *Dendrite* factors. However, "most important[]" was whether plaintiffs made "an adequate showing" of their claims. The court noted the differing standards from the cases "on what constitutes such an adequate showing," including standards "fairly deferential to the plaintiff" of "a 'good faith basis'" or "probable cause"; a motion to dismiss standard, or a higher summary judgment standard; and "a concrete showing as to each element of a prima facie case." *Doe I* adopted the "concrete showing" standard. "[S]uch a standard strikes the most appropriate balance between the First Amendment rights of the defendant and the interest in the plaintiffs of pursuing their claims…." Concluding that plaintiff met this standard, the court denied the motion to quash.

Two subsequent decisions highlight the uncertainty of the disclosure test. In *Ottinger v. Journal News*,[13] petitioners sought the identities of website bloggers. Relying on *Dendrite*, the court held that a plaintiff must give an anonymous speaker notice and an opportunity to be heard; set forth the exact statements; establish a "prima facie" cause of action with "sufficient evidence" supporting each element; and show that the strength of the prima facie case and the need for disclosure outweigh the right to anonymity. On these considerations, the court authorized disclosure.

Cohen v. Google Inc.,[14] however, took a different tack. Petitioner sought identifying information from Google for an anonymous blogger who posted allegedly defamatory comments. The court focused simply on the two traditional Section 3102(c) requirements, finding that petitioner had "sufficiently established the merits of her proposed cause of action for defamation" and that "the information sought [was] material and necessary to identify the potential defendant."

The *Cohen* court, however, did not look to a multi-factor balancing test. Rather, it stated that the New York law "generally applicable to a CPLR 3102(c) application…which requires a prima facie showing of a meritorious cause of action, and the legal requirements for establishing a meritorious cause of action for defamation, appears to address the constitutional concerns." Significantly, the court rejected the blogger's argument that the Internet context of the allegedly defamatory statements—that blogs have evolved into the "modern day soapbox for one's personal opinions"—changed the factual nature of the statements into non-actionable opinion.

Most recently, the First Department in *Sandals Resorts International Ltd. v. Google Inc.*[15] upheld the denial of pre-action disclosure seeking the identity of an unknown gmail account-holder who allegedly wrote a defamatory e-mail. It found that petitioner failed to show a meritorious defamation claim since the statements were not false statements of fact; petitioner did not properly allege injury; and the statements were protected opinion. Petitioner therefore did not meet even the first prong for pre-action disclosure—which the court determined without referring to a specific standard for showing a meritorious claim. Consequently, the court also did not reach the multi-factor balancing test.

Interestingly, *Sandals* accepted that the Internet gives speech a different character for assessing defamation claims. "[T]he anonymity of the e-mail makes it more likely that a reasonable reader would view its assertions with some skepticism and tend to treat its contents as opinion rather than as fact." The First Department explained that while e-mail disseminating injurious falsehoods is not immunized, courts nonetheless "should protect against '[t]he use of subpoenas by corporations and plaintiffs with business interests to enlist the help of ISPs via court orders to silence their online critics[, which] threatens to stifle the free exchange of ideas.'" Whether this perception affects pre-action disclosure of an anonymous speaker's identity will need to play out in future cases.

Ramifications, Best Practices

An objectionable, anonymously written post appears on a widely viewed website, or by an e-mail, about your client; or it's your client's website, or perhaps it was your client who authored the post. What's next?

The aggrieved party might seek disclosure of the speaker's identity by commencing a Section 3102(c) special proceeding. But the threshold question of from whom to seek disclosure might not be straightforward. Where comments come directly from a known IP address, the ISP can be determined, and the ISP usually can identify its subscriber—so disclosure should be sought from the ISP. But for statements on a website, the website itself might be hosted through a series of providers, so the entity that knows the speaker's identity could be hard to determine.

Further investigation before filing under Section 3102(c) might be necessary to trace participants in the chain of communications. For example, counsel can contact the known website host to lodge a complaint and seek information on the speaker's identity. Sometimes that entity will identify its provider, allowing counsel to get closer to identifying the speaker. Often an expert, such as an investigative services firm, can assist in unraveling the cyberspace chain. Where layers of hosting entities or providers exist, the objective is to bring the proceeding against an entity most likely to possess the speaker's identity. However, sometimes it might be appropriate to name several entities to try to unmask the speaker.

Where layers of hosting entities or providers exist, the objective is to bring the proceeding against an entity most likely to possess the speaker's identity. However, sometimes it might be appropriate to name several entities to try to unmask the speaker.

Personal jurisdiction might also be an issue. Where the party thought to possess the identifying information is a large ISP or other provider serving a major market, its presence or contacts for New York in personam jurisdiction might be a given. But where the host provider for a website is based elsewhere, exercising jurisdiction in New York could be problematic.

Assuming an appropriate respondent is identified, petitioner can seek Section 3102(c) relief by order to show cause to expedite the application. The request might include a temporary restraining order/preliminary injunction requiring respondent to preserve relevant documents and electronically stored information (such as an ISP's subscriber information for a particular IP address). However, even absent a request for injunctive relief, the respondent would be well advised to preserve the information, akin to a legal hold situation.

The application should include specific information for the identification process as determined by petitioner's investigation. For example, petitioner should set forth what he (or his expert) has done to track the objectionable statements to electronic source information (IP addresses/time of communication, ISP or hosting provider of the communication, website sponsor, etc.) and specify how that information enables respondent to identify the speaker from its records.

Importantly, petitioner should be prepared to give notice to the anonymous speaker. This might involve posting notification of the application on the website, message board or blog where the objectionable statement originated, with particulars about the right to be heard. Some providers also have a policy of advising a subscriber when a subpoena or process issues for subscriber information. That policy can be significant because it undercuts a subscriber's privacy expectation, which is often considered in the balancing equation. Indeed, ISPs and other providers should consider their subscriber privacy provisions and service agreements with this in mind, since the policy makes it more likely they will be required to disclose a subscriber's identity.

Finally, the merits of the proposed claim arising from the objectionable speech are critical. A petitioner should be prepared to show that the claim meets an exacting standard, although there is leeway in the cases that rely on a less rigorous showing. Similarly, whether the Internet's unique character will affect the perceived strength of a claim, particularly for defamation, may be important. In any event, a petitioner should spell out the allegations underlying the proposed claim; while a proposed complaint is not required on a Section 3102(c) application, in some situations it might be advisable to include one.

In short, whether a cyberspace speaker can maintain anonymity in the face of someone else's objections to the speech remains a challenging issue for future cases.

1. *Liberty Imports Inc. v. Bourguet*, 146 A.D.2d 535, 536 (1st Dept. 1989).
2. *Stewart v. New York City Transit Auth.*, 112 A.D.2d 939, 940 (2d Dept. 1985).
3. *Dublin Worldwide Prods. (USA) Inc. v. Jam Theatricals, Ltd.*, 162 F.Supp.2d 275, 277 (S.D.N.Y. 2001).
4. *In re Vioxx Prods. Liab. Litig.*, 2008 WL 1995098 (E.D. La. May 6, 2008); *In re Landry-Bell*, 232 F.R.D. 266 (W.D. La. 2005); but see *In re Alpha Indus. Inc.*, 159 F.R.D. 456 (S.D.N.Y. 1995).
5. See *Digiprotect USA Corp. v. Does* 1-266, 2011 WL 1466073 (S.D.N.Y. April 13, 2011).
6. 47 U.S.C. §230(c)(1).
7. 326 F.Supp.2d 556 (S.D.N.Y. 2004).
8. The U.S. Court of Appeals for the Second Circuit adopted the *Sony* standards in *Artistic Records LLC v. Doe 3*, 604 F.3d 110 (2d Cir. 2010).
9. 8 Misc.3d 820 (Sup. Ct. New York Co. 2005).
10. 18 Misc.3d 185 (Sup. Ct. New York Co. 2007).
11. 342 N.J. Super. 134 (Super. Ct. App. Div. 2007).
12. 561 F.Supp.2d 249 (D. Conn. 2008).
13. 2008 N.Y. Misc. LEXIS 4579 (Sup. Ct. Westchester Co. June 27, 2008).
14. 25 Misc. 3d 945 (Sup. Ct. New York Co. 2009).
15. 86 A.D.3d 32 (1st Dept. 2011).wp