Reprinted with permission from the July 23, 2001 *New Jersey Law Journal*.

Intellectual Property

Grappling With 'Cybersmear'

Right to protection from cybersmear is balanced against the perceived First Amendment rights of anonymous Internet 'posters'

By Peter J. Pizzi

The perceived anonymity of the Internet emboldens many users to publish messages they may not otherwise have sent if the messages could be attributed to them. New Jersey's Appellate Division has become the first appellate court in the nation to set forth comprehensive procedures applicable to "cybersmear" suits, where the plaintiff seeks to discover the identity of persons posting defamatory or actionable messages on the Internet.

The decisions in *Dendrite International, Inc. v. John Doe*, No. 3, A-2774-00T3 (July 11, 2001), and *Immunomedics, Inc. v. Jean Doe*, a/k/a/ "moonshine_fr," A-2762-00T1 (July 11, 2001), specify how plaintiffs may obtain pre-service discovery to identify posters and the standards courts must apply to such requests.

The two opinions struggle to balance a plaintiff's right to protect itself from cybersmear against perceived First Amendment rights of the poster to remain anonymous. Indeed, the two opinions serve to counterbalance each other. Whereas *Dendrite* makes it more difficult to unmask posters based on defamation claims, *Immunomedics* offers hope to companies seeking to stop former employees from disclosing proprietary information in Internet chat rooms.

Cybersmear

Cybersmear proliferates today because of three defining qualities of the Internet itself. First, the Internet is ubiquitous. Information posted on the Internet may be accessed from everywhere in the world instantaneously.

Second, the Internet creates the illusion of anonymity. Just as users browse Web sites without having to reveal their identity, visitors to chat rooms post messages anonymously or, at least, pseudononymously in a myriad of Internet sites. Most Internet forums only require the user to create a pseudonym or, in the lexicon made popular by America OnLine, a "screen name." This anonymity is illusory, however, because every Internet message or mouse click leaves a digital trace that can be followed to the source computer.

Third, the Internet is eternal, or nearly so. Message boards retain a historic record of posted messages; most have online archives of messages that are instantly searchable. Thus, a defamatory posting remains accessible by any one of hundreds of Internet search engines months and years after its original date of posting. This can be the case even if the message was removed in response to a complaint. Many search engines, such as www.google.comhttp://www.google.com/, retrieve not only live Web site pages but also "cached" versions of pages that have been removed from the server that first offered the material to the world.

These three traits -- ubiquity, the illusion of anonymity and eternity -- are what most vex companies when they learn that they have been a victim of cybersmear.

News accounts of cybersmear cases have mostly involved publicly held companies suing anonymous Internet posters over messages on financial Web sites such as those offered by Yahoo Finance, Motley Fool, AOL, CNBC and other Web portals. These sites offer a vast array of information, including Securities and Exchange Commission filings, stock charts, press releases and, most pertinent here, message boards where surfers can post comments about goings-on in the company. Such message boards serve as the forum for angry former employees to seek revenge against their former employer or against particular former colleagues.

One of the most extreme examples is www.****edcompany.com, a site that the investment community follows closely for clues about how technology companies are weathering the Internet bust. (The asterisks replace a very bad four-letter curse word.)

This site aims to attract insiders working at dot-coms that are on their way to becoming dot bombs and to elicit revelations about how bad things really are at the company. The ****edcompany.com board creates a "deadpool" in which participants predict how soon a dot-com, telecom or other technology firm will meet its

demise. The site's message boards are actually dubbed the "Happy Fun Slander Corner."

But privately held companies can also become cybersmear victims simply because the Internet offers limitless places in which messages on any topic can be posted and read by those sharing an interest in that topic. Usenet newsgroups and Internet Web sites abound that focus on particular industries or technologies.

At www.vault.com, which dubs itself an "electronic watercooler," employees at companies both large and small are encouraged to rant (and even sometimes rave) about their experience at a current or former job. Thus, postings frequently contain complaints that denounce particular supervisors by name, accusing them of incompetence and sometimes of outright discrimination. Needless to say, such charges, if groundless and made maliciously to seek revenge on the former employer, can motivate the victim to seek redress.

Unmasking the Poster

Corporations trying to put a stop to cybersmear find that a few New Jersey court rules can be called on to provide a remedy.

First, Rule 4:26-4 permits suit to be filed against the defendant under a fictitious name where the defendant's true name is unknown. Once the true name of the defendant is determined, the plaintiff must amend the complaint accordingly.

The Federal Rules of Civil Procedure are silent on fictitious defendants, but case law supports the same procedure. Federal courts have long approved the use of fictitious names for defendants even without discussion. See *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*, 403 U.S. 388 (1971).

Most cybersmear cases are filed in state court, however, because it is impossible to plead diversity of citizenship against a defendant whose identity and residence are unknown and because a basis for federal question jurisdiction is generally lacking.

Once a complaint is filed, the plaintiff corporation must then file an application for leave to conduct discovery before the service of a summons. Rule 4:14-1 requires litigants to obtain leave of court to propound discovery prior to the expiration of 35 days after service of the summons and complaint. In fact, prior to *Dendrite*, many corporate plaintiffs simply served the subpoena after filing the complaint, without obtaining leave of court at all.

The discovery that companies use to unmask the identity of anonymous Internet posters is a subpoena directed to AOL, Motley Fool, Yahoo or other Internet service providers or Web portals. Such subpoenas seek documents containing any identifying information about the pseudonym under which the postings were made. If the poster made his postings in an AOL financial chat room, he or she presumably would have an AOL account, and AOL could be subpoenaed to disclose the account information.

This AOL account information is generally accurate because AOL is a pay service and the name given must match that of the credit card used to pay for the service. On the other hand, free portals such as Yahoo may not receive accurate account information when users create login names. If the account information is not accurate, the plaintiff must trace the "IP" information -- the computer addresses that identify the computer or network from which the message originated -- to a particular user at the time of the posting. That requires additional subpoenas.

On receipt of such subpoenas, AOL, Yahoo and other ISPs or Web portals send an e-mail to the poster giving notice that a subpoena had been served on it to produce documents revealing his or her identity and advising of the particulars of the case should the poster desire to intervene to oppose the relief.

Most often, the poster ignores the e-mail, the documents are produced and the plaintiff then files an amended complaint naming the poster as a defendant using his or her true identity. The case then proceeds like any other civil action.

Providing a Roadmap

Through the *Dendrite* and *Immunomedics* decisions announced July 11, 2001, the Appellate Division changed the procedural landscape applicable to cybersmear suits.

The facts in *Dendrite* began in the spring of 2000, when Dendrite International, Inc., which produces software for the pharmaceutical industry, found itself afflicted by anonymous postings on the "DRTE" Yahoo Finance Board. Among other things, the messages alleged that the corporation's chairman was "shopping" the company and that he had used various techniques to improve year-end financial results.

Dendrite sued the posters in Morris County and named John Does Nos. 1 through 4 as defendants, alleging claims of misappropriation of trade secrets, breach of contract and fiduciary duty, and defamation.

Before ruling on Dendrite's request to serve a subpoena on Yahoo, Judge Kenneth C. MacKenzie ordered Dendrite to post a notice of the application on the DRTE Board itself. On June 23, 2000, Dendrite complied. As evidence of the eternity of the Internet, that notice still appears on the DRTE Board as message no. 867, along with the chatter from other posters that the notice provoked.

In response to the notice, John Does Nos. 3 and 4 each retained counsel to oppose Dendrite's application. John Does Nos. 1 and 2 did not appear or contest the relief. The Washington D.C.-based Public Citizen Litigation Group, originally founded by Ralph Nader, appeared as an amicus to oppose Dendrite's application.

In a lengthy opinion issued on Nov. 23, 2000, Judge McKenzie followed a four-part test developed in *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999), in which the plaintiff sought to unmask a cybersquatter. Judge McKenzie also discussed at some length the Virginia lower court decision, *In Re Subpoena Duces Tecum to America Online, Inc.*, 2000 WL 1210372 (Va. Cir. Ct. Jan. 21, 2000), rev'd on other grounds sub. nom. *America Online, Inc. v. Anonymous Publicly Traded Company*, 542 S.E.2d 377 (Va. 2001), in which the plaintiff corporation sought to proceed anonymously in an action alleging cybersmear on the part of several "John Doe" defendants; thus both sides were anonymous.

Both *Seescandy.com* and *AOL* held that the right to discovery must be balanced against a citizen's right to speak anonymously. At first blush, this might seem a dubious proposition. Why does free speech extend to a right to speak without disclosing one's identity? The Internet would perhaps be a much safer place for everyone if Internet messages could be attributed to the true author.

The lower court in *AOL*, however, pointed out that anonymous speech has an impressive pedigree in American history. The court noted that even the Federalist Papers had been published by James Madison, Alexander Hamilton and John Jay under the pseudonym "Publius."

Based on the premise that the right to speak anonymously is protected by the First Amendment, the court in *Seescandy.com* held that a plaintiff seeking to unmask the author of anonymous Internet messages must satisfy four discrete criteria.

First, a plaintiff must "identify the missing party with sufficient specificity such that the Court can determine that the defendant is a real person or entity who can be sued in federal court."

Second, all the steps taken in the plaintiff's attempt to locate the defendant must be illustrated. This element is easily satisfied because Yahoo, AOL and most other ISPs resist disclosing the identity of users unless required by compulsory process.

Third, the plaintiff must establish that its suit "could withstand a motion to dismiss." This is necessary to "prevent abuse of this extraordinary application of the discovery process and to ensure that plaintiff has standing to pursue an action against defendant."

And fourth, the plaintiff must file the discovery request with the court and show that the discovery is narrowly crafted to yield only information identifying the poster.

Though Judge MacKenzie professed to apply the *Seescandy.com* four-part analysis, he actually required that Dendrite first prove a prima facie case before it could obtain discovery to identify the defendant. On the issue of "actual reputational injury," a required element of Dendrite's defamation claim (the only potentially viable claim against John Doe No. 3), Judge MacKenzie was not satisfied with mere allegations of injury:

> It is not obvious that the statements at issue are false or that Dendrite has been harmed. Dendrite has failed to show that the messages in question in any way harmed Dendrite. Although Dendrite alleges that it has been harmed and that it will continue to be harmed by the defendants' statements, saying it is so does not make the allege harm a verifiable reality.

Based on this analysis, Judge MacKenzie held that Dendrite did not have colorable claims against John Does Nos. 3 and 4 and therefore denied Dendrite discovery against them, effectively dooming its claim against those defendants.

In its opinion on July 11, 2001, the Appellate Division affirmed the procedure followed and the standards applied by Judge MacKenzie. The court held that rights afforded by

the First Amendment remain protected even when engaged in anonymously. As a result, courts must balance the plaintiff's right to protect its reputation and proprietary interests against the poster's First Amendment right to maintain his or her anonymity.

In terms of procedure, the Appellate Division held that, henceforth, an order granting leave to pursue discovery that would breach a poster's anonymity may not be entered until after the plaintiff has "undertake[n] efforts" to notify the anonymous poster of the application. The plaintiff must at the very least post a notice of the application on the Internet forum used by the poster:

> We hold that when such an application is made, the trial court should first require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, and withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application. These notifications efforts should include posting a message of notification of the identity discovery request to the anonymous user on the ISP's pertinent message board.

In addition, before allowing the discovery, the motion judge must perform an analysis of the plaintiff's case beyond that required on a traditional motion to dismiss. The plaintiff must prove a prima facie right to recovery and "sufficient" evidence to support each element of its claim:

> In addition to establishing that its action can withstand a motion to dismiss for failure to state a claim upon which relief can be granted pursuant to Rule 4:6-2(f), the plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant.

Last, the Appellate Division ruled that, even if the court concludes that the plaintiff's case passes muster under these criteria, the court must then balance the First Amendment right of anonymity of the poster against the strength of the prima facie case presented and the need for the discovery:

> Finally, assuming the court concludes that the plaintiff has presented a prima facie cause of action, the court must balance the defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed.

The court then applied these standards to Dendrite's request to unmask John Doe No. 3, whose postings stated that the corporation's chairman was shopping the company and that he changed the company's revenue recognition practice. The court conceded that the claims would survive a motion to dismiss, but still affirmed Judge MacKenzie's conclusion that Dendrite had not proved these statements caused the company harm:

> The record does not support the conclusion that John Doe's postings negatively affected the value of Dendrite's stock, nor does Dendrite offer evidence or information that these postings have actually inhibited its hiring practices, as it alleged they would. Accordingly, the motion judge appropriately concluded that Dendrite failed to establish a sufficient nexus between John Doe No. 3's statements and Dendrite's allegations of harm.

Immunomedics

The corporate plaintiff in *Immunomedics* fared much better. In that case, the anonymous poster, who went by the Internet handle "moonshine," claimed to be a "worried employee" of the company. Her Yahoo postings disclosed that the company was out of stock in a key product in Europe and was about to fire the manager in that region. Immunomedics sued moonshine, alleging breach of contract and served a subpoena on Yahoo, apparently without first applying for leave. Consistent with its practice, Yahoo e-mailed moonshine to alert her to the Morris County suit, and moonshine, proceeding anonymously, moved to quash the subpoena.

Immunomedics conceded that the statements were true but asserted that moonshine had violated the company's confidentiality agreement and "several provisions" of the company's employee handbook. On the record before her on moonshine's motion to quash, Motion Judge Zucker-Zarett had nothing to contradict the allegation that moonshine was bound by the confidentiality agreement and,

therefore, denied moonshine's motion to quash. Moonshine's appeal of that order became a companion case to *Dendrite*.

The Appellate Division affirmed, holding that the motion judge properly balanced moonshine's First Amendment interest in remaining anonymous against the company's right to protect confidential business information from disclosure:

> Although anonymous speech on the Internet is protected, there must be an avenue for redress for those who are wronged. Individuals choosing to harm another or violate an agreement through speech on the Internet cannot hope to shield their identity and avoid punishment through invocation of the First Amendment.

Striking a Balance?

At first glance, the criteria enunciated in *Dendrite* may appear as overkill when all that is sought is the right to issue a subpoena to find out who the defendant actually is. *Immunomedics* suggests that application of these criteria will not prove insurmountable for employers seeking to stop offending messages by former employees, particularly where suitable workplace agreements are in effect.

The opinions raise some interesting issues involving the interplay between the law of defamation, the First Amendment and traditional rules of civil procedure. Under *Dendrite*, in order for the plaintiff to serve discovery to uncover the defendant's identity, it is not enough that the complaint state a proper cause of action for defamation. Instead, that plaintiff must first submit proofs to make out a prima facie case, which is essentially the threshold needed to survive a motion for summary judgment.

By contrast, under *Printing Mart-Morristown v. Sharp Elect. Corp.*, 116 N.J. 739 (1989), a motion to dismiss will be denied so long as "the fundament of a cause of action may be gleaned" from the complaint. See also *Brill v. Guardian Life Ins. Co. of America*, 142 N.J. 520 (1995); and Pressler, Current N.J. Court Rules (Gann), Comment on Rule 4:46-2.

Dendrite, thus, raises the question why the traditional motion to dismiss standard applicable to defamation cases is insufficient when the defendant's identity happens to be unknown and the forum for the message happens to be the Internet.

The appellate panel in *Dendrite* felt free to depart from *Printing Mart* and instead looked to *Seescandy.com*, which likened pre-service discovery to a search warrant and suggested that a showing akin to probable cause should be made. And because a pre-service application for discovery lies within the discretion of the court, the Appellate Division apparently elected to craft a new procedural mechanism, not covered by New Jersey's court rules, in order to guide judges in the exercise of that discretion.

The court in *Dendrite* justifies the more rigorous burden imposed on the plaintiff by pointing to the First Amendment implications of exposing the true identity of anonymous posters in Internet chat rooms. However, no one who posts messages on Internet message boards proceeds with true anonymity. Every computer-generated message leaves a trace that can be followed to identify the author. The Internet is, after all, merely a computer network.

Thus, those who post to message boards necessarily encounter the risk that their identity will be discovered by someone with the motivation to do so. Just as the threat of product liability actions may be said to encourage safer products, the availability of discovery devices to unmask those responsible for cybersmear likewise may serve to discourage the transmission of irresponsible postings on the Internet.

Dendrite also suggests that even where the plaintiff has made the required prima facie showing, the motion judge may still exercise discretion to deny discovery needed to unmask the poster under the guise of achieving a balance between the First Amendment rights of the anonymous defendant and those of the plaintiff to seek redress for perceived wrongs. It is not clear from the opinion what criteria lower courts are to apply in addressing this last element of the *Dendrite* analysis.

Like many courts addressing issues spawned by the Internet, the panel in *Dendrite* was proceeding in uncharted territory. For that reason, it felt free to jettison traditional criteria applied to test the legal sufficiency of a defamation complaint and develop a new rubric that aims to balance the plaintiff's interests against the First Amendment interests of the anonymous Internet poster.

Dendrite creates some additional hurdles before a victim of cybersmear may identify the person responsible for the offending message. Application of those criteria in *Immunomedics*,

however, suggests that judicial outcomes may not vary widely from the way in which New Jersey judges had been handling such cases over the past few years.

The author is a certified civil trial attorney and chair of the Internet and information technology practice group at Connell Foley LLP of Roseland.