PROSKAUER ROSE®

Client Alert

A report
for clients
and friends
of the firm

January 2002

"Cybersmearing" Remedies: Companies Seeking to Unmask Anonymous Online Enemies Should Proceed Carefully

The Internet is a medium where people can "get even." Employees and, more frequently, ex-employees who feel aggrieved by their workplace treatment can post anonymous, libelous statements about their boss, the CEO and the company. Or they can share corporate secrets or spread false rumors affecting the company's financial position, all the while maintaining anonymity on the Internet. Often the harm is nothing more than bruised executive egos; sometimes, however, the harm is tangible and serious. Rumors about a corporation's financial standing can snowball into a financial crisis in certain situations.

When "cybersmearing" (online defamation) occurs, or disclosures of non-public information are made online, the first goal is to get the culprit to stop using the Internet to harm the company. But how do you get the wrongdoer to stop if you don't know who he or she is? One way is to file a full-blown lawsuit against a "John Doe," and then take discovery to determine the identity of Mr. or Ms. Doe. Lawsuits cost money and take time, and the delay between filing and discovery may be too protracted for effective relief from the online defamation or publication of trade secrets.

Another route is to use judicial procedures to identify wrongdoers in proceedings designed to avoid full-blown lawsuits. But even such streamlined procedures can present legal hazards, as some recent decisions have shown. It has gotten harder to discover the identities of online wrongdoers, as the First Amendment has been invoked as a shield against unmasking.

Companies considering litigation to determine the identity of an anonymous (or pseudonymous) online actor should take note of two decisions by a New Jersey appellate court and a decision by a federal court in Washington State, which illustrate the First Amendment considerations in resolving a plaintiff's right to compel identification of an anonymous Internet speaker. The courts recognize the need to unmask irresponsible online publishers but also are aware of the right to express oneself, even anonymously, a right that has its roots in the anonymous pamphleteering of Thomas Paine.

While an unknown Internet speaker's identity may be obtained through the use of subpoenas, plaintiffs often must make a showing of entitlement before disclosure will be ordered. What this means, in the end, is that a litigant must show its claim is real and not just a device to silence an unwanted critic. Understanding the emerging legal landscape will assist in evaluating whether to bring litigation, and the potential pitfalls.

The New Jersey Decisions

In two opinions issued the same day, the Appellate Division of the Superior Court of New Jersey outlined standards which courts should apply when considering a plaintiff's request to compel disclosure of the identity of an anonymous Internet defendant. Using these standards, the court denied the request for disclosure in one case, and in the other, granted the application.

In *Dendrite International, Inc. v. John Doe*, No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001), the court denied Dendrite Corporation's application for discovery of the identity of a defendant from Yahoo!, Inc. Dendrite, a publicly traded corporation, alleged that a series of postings by anonymous individuals (identified as "John Does 1-14") to a Yahoo! message board dedi-

In this issue:

cated to discussion about the company were defamatory, were made in breach of contractual obligations owed to the company and misappropriated trade secrets. At issue in the appeal was whether Dendrite could compel identification of Doe No. 3 based on its contention that the statements constituted actionable defamation.

Doe No. 3 was alleged to have made a series of nine postings, several of which criticized a purported change in Dendrite's accounting and revenue recognition procedures, its president's conduct, and alleged that the company was not progressing competitively and that efforts to sell the company had been unsuccessful. In support of its defamation claim, Dendrite submitted testimony that Doe No. 3's statements were substantively false, and that the postings had damaged the company's stock price. The trial court denied the request for disclosure, finding that plaintiff had not made out a *prima facie* case. The appellate court affirmed the ruling, finding that the trial court had struck the proper balance between Doe's First Amendment right to speak anonymously and Dendrite's right to protect its proprietary interests and reputation.

The appellate court listed the following requirements for the issuance and enforcement of a subpoena to identify the wrongdoer:

1. Plaintiff needs to provide reasonable notice to the anonymous poster that he or she is the subject of an application for disclosure (*e.g.*, by posting to the forum where the individual's statements appeared);

2. Plaintiff must identify specifically the statements at issue alleged to constitute actionable speech;

3. Plaintiff must set forth a *prima facie* cause of action, including an evidentiary demonstration of each element of the alleged cause of action. Once plaintiff has set forth a *prima facie* case, the court should balance the defendant's First Amendment right to speak anonymously against the strength of plaintiff's case and her need for disclosure to proceed properly.

Of these factors, the main issue in contention in *Dendrite* was the third factor. The trial court found that, prior to obtaining discovery of an anonymous defendant's identity, the plaintiff seeking the identification must plead the substantive claims underlying the request — *i.e.*, the wrongs allegedly committed by the anonymous individual — sufficiently to withstand a motion to dismiss. However, the court analyzed Dendrite's underlying claims under more exacting standards than those generally applied to evaluate dismissal motions.

Affirming the trial court's decision, the appellate court analogized Dendrite's request for identification to an *ex parte* request by the government to a court for a criminal search warrant, and concluded that the standards for evaluating an identification request should be similar to the "probable cause" standard employed in the criminal context. It found, as a Virginia court had in a case involving America Online, that strict standards were necessary to ensure that plaintiffs would not abuse the discovery process to "harass, intimidate or silence critics in the public forum opportunities provided by the Internet."

On the same day it issued the *Dendrite* decision, the New Jersey court affirmed a decision to permit discovery of an anonymous defendant's identity in *Immunomedics, Inc. v. Jean Doe*, 775 A.2d 773 (N.J. Super. Ct. App. Div. 2001). Immunomedics sued an anonymous individual who posted to a Yahoo! message board, alleging that the defendant's postings were made in breach of contract, in breach of the duty of loyalty, and negligently revealed the company's confidential and proprietary information. Immunomedics subpoenaed Yahoo! for information identifying the defendant. The defendant sought, anonymously through counsel, to quash the subpoena.

The pseudonymous defendant in *Immunomedics* claimed to be a "worried company employee." Her postings alleged that the company was out of stock for certain products in Europe and that the company intended to fire its European manager. In its application to discover the defendant's identity, Immunomedics conceded that the information contained in the postings was true. However, the company testified that all its employees were required to sign a confidentiality agreement that forbade

Recent Developments in Privacy Law: FTC Says Online Policies Apply Offline

Implications for Business May Be Significant

The Federal Trade Commission's Consumer Protection Bureau has signaled that privacy protections announced online (in Web Sites, for example) may apply to consumer information collected offline. This expansive view of privacy protection may impose significant obligations on businesses.

Recent statements made by the Director of the FTC Bureau of Consumer Protection indicate that a company's collection of data about individuals in the offline world should conform to the company's privacy policies posted on its Web Site.

Apart from children's privacy, financial institution data, and data coming from the European Union, there is no general obligation for a company even to have a privacy policy. But most companies have adopted or are adopting such policies in

the disclosure of such information, and that the disclosures also violated certain company policies described in its employee handbook.

Applying the same standards articulated in *Dendrite*, the court found that Immunomedics did establish a *prima facie* case under the causes of action it alleged. The trial court found that Jean Doe was an employee, and in that context had contracted to abide by certain limitations on her speech concerning the company. The court thus found that Immunomedics was entitled to identify her and to pursue its claims:

> Although anonymous speech on the Internet is protected, there must be an avenue of 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 though invocation of the First Amendment.

The court rejected Doe's argument — which has been made by several defendants in such cases — that she should first be allowed to disprove plaintiff's claims while maintaining anonymity, and that disclosure of her identity only could be compelled if she did not defeat plaintiff's claims. It found that Doe was not entitled to a more advantageous position based upon either the medium in which she chose to commit the breach of contract or because she did so anonymously.

light of the significant public interest in privacy protection. The FTC has authority to ensure that promises made about privacy are kept. (A misrepresentation could result in liability under Section 5 of the FTC Act.)

To date, FTC privacy policy enforcement actions have centered largely on companies that do not follow their posted privacy practices with respect to consumer data collected online. Under its newly announced direction, if information collected about consumers offline is used in ways that contravene a company's posted privacy policy, the Agency may view the company's information practices as deceptive. The FTC did not address whether or how it might account for differences in a company's online and offline businesses and collection of consumer data.

It is unclear how the FTC intends to implement this new enforcement policy. In light of the Agency's statements, companies should evaluate whether the consumer information they collect offline is handled in accordance with their posted privacy policies and, if not, whether and how to change "land-based" (offline) practices or limit the reach of the posted policies.

Proskauer lawyers are available to consult on this compliance issue.

The Washington State Decision

The United States District Court for the District of Washington similarly resolved a discovery contest about whether a litigant could obtain the identities of twenty-three non-parties who made pseudonymous postings to a bulletin board service maintained by the Seattle-based Internet company, InfoSpace, Inc.

In *Doe v. 2Themart.com, Inc.*, 140 F. Supp. 2d 1088 (W.D. Wa. 2001), shareholders of 2Themart.com sued the company and its directors for alleged securities fraud. Among the defenses raised by the company was that the fluctuations in its stock price that were the subject of the shareholder action were not caused by the board of directors, but instead were the result of numerous and damaging postings made by pseudonymous individuals to an InfoSpace bulletin board allegedly for the purpose of manipulating the company's stock price. 2Themart.com subpoenaed the identities of the individuals from InfoSpace. InfoSpace notified the individuals whose identities were sought, and one proceeded to challenge the subpoena anonymously.

The federal court concluded that the standards for compelling the identification of a non-party witness required the application of even higher standards than when disclosure of a party's identity is sought. It found that "[n]on-party disclosure is only appropriate in the exceptional case where the compelling need for the discovery sought outweighs the First Amendment rights of the anonymous speaker." The court derived a four-part test, requiring that the party seeking disclosure must show:

1. That it seeks the information in good faith;
2. The information relates to a core claim or defense in the action;
3. The identification is directly and materially relevant to a core claim or defense in the action; and
4. Information sufficient to establish or rebut the core claim or defense is unavailable from any other source.

Based on these standards, the court quashed 2Themart.com's subpoena. While the court allowed that the subpoena may have been brought in good faith, it found that the information sought did not relate to a core claim or defense, but instead was one of only twenty-seven affirmative defenses raised. The court further cautioned that, prior to identification, the information must be shown to directly and materially relate to the requesting party's claim or defense to be discoverable because "when First Amendment rights are at stake a higher threshold of relevancy must be imposed." *Id.* at 1096. The court determined that the anonymous third parties' identities were not directly and materially relevant to 2Themart.com's claims and defenses, as the third parties were not defendants to any claim, cross-claim or third-party claim. The court also concluded that the information 2Themart.com needed for its defense was available

to it without identifying the third-party posters and, thus, that 2Themart.com could support its defense without encroaching on the First Amendment rights of the posters.

Notably, the court acknowledged that many civil subpoenas to ISPs will be complied with without notice to the user whose identity is sought, and without challenge by the ISP. However, the court did not, as the New Jersey courts, require prior notification to the anonymous user.

Litigation Considerations

Anonymous online publishers have been given more explicit rights in recent court decisions, making it harder to unmask wrongdoers absent a full-blown litigation. As the recent decisions make clear, clients who have been harmed by individuals acting anonymously online do have recourse to discover the identities of the responsible individuals and to hold them accountable for their conduct. However, decisions to litigate should be reviewed carefully to determine whether the evidence of wrongdoing will satisfy the high discovery threshold increasingly being applied by the courts. As well, clients should consider and be prepared to meet adverse publicity that could result from a decision to pursue anonymous tortfeasors, many of whom can find legal and financial support from organizations, including ISPs, that have challenged and even filed successful counterclaims in response to disclosure requests.

Has Your Address Changed?

Please let us know if your mailing address needs to be updated. Contact Deborah Chernoff with the correct information either via e-mail: dchernoff@proskauer.com or fax: 212.969.2900.

You can also visit our Website at **www.proskauer.com**

NEW YORK LOS ANGELES
WASHINGTON BOCA RATON
NEWARK PARIS

Client Alert

For further information on this or other Internet legal issues, please contact:

Christopher Wolf
202.416.6818 - cwolf@proskauer.com

Amybeth Garcia-Bokor
202.416.6869 - agarcia-bokor@proskauer.com

Proskauer is an international law firm with more than 540 attorneys who handle a full spectrum of legal issues worldwide.

1585 Broadway
New York, NY 10036-8299
212.969.3000

2049 Century Park East
32nd Floor
Los Angeles, CA 90067-3206
310.557.2900

One Newark Center
18th Floor
Newark, NJ 07102
973.274.3200

68, rue du Faubourg Saint-Honore
75008 Paris, France
331.53.05.60.00

1233 Twentieth Street, NW
Suite 800
Washington, DC 20036-2396
202.416.6800

One Boca Place
Suite 340 West
2255 Glades Road
Boca Raton, FL 33431-7383
561.241.7400

PROSKAUER ROSE
Produces Results℠

1585 Broadway
New York, NY 10036-8299
212.969.3000

2049 Century Park East
Suite 3200
Los Angeles, CA 90067-3206
310.557.2900

2255 Glades Road
Suite 340 West
Boca Raton, FL 33431-7360
561.241.7400

1233 Twentieth Street NW
Suite 800
Washington, DC 20036-2396
202.416.6800

One Newark Center
18th Floor
Newark, NJ 07102-5211
973.274.3200

68 rue de Faubourge Saint-Honoré
75008 Paris, France
33.1.53.05.60.00

www.proskauer.com