Journal of Information, Law and Technology

Cybersmearing: A Legal Conflict Between Individuals and Corporations

Gregory J. Naples
Associate Professor
Department of Accounting
Marquette University
Milwaukee USA
gregory.naples@marquette.edu <mailto:gregory.naples@marquette.edu>

Meredith Maher
Graduate Research Assistant
Department of Accounting
Marquette University
Milwaukee USA
meredith.maher@marquette.edu

This is a **refereed** article published on: 16 August 2002

Citation: Naples G J and Maher M, 'Cybersmearing: A Legal Conflict between Individuals and Corporations' *The Journal of Information, Law and Technology (JILT)* 2002 (2) <http://elj.warwick.ac.uk/jilt/00-3/naples.html>

Abstract

Cybersmearing is the act of anonymous communication of false information about a corporation over the Internet, which causes economic damages. Initially, Internet Service Providers (ISPs) were concerned with their legal liability, which was limited by the Communication Decency Act of 1996. Next, courts in the United States struggled with how to compensate corporations from the anonymous acts. The courts issued subpoenas to the ISPs to determine the true identity of the anonymous user and then proceed with the case. However, currently the federal and state courts in the United States are struggling with the balance between Internet privacy and corporate defamation. First Amendment rights ensure that Internet users can communicate freely; however, United States Tort law ensures that corporations have the right to protect their reputations. Hundreds of cases have been filed relating to this topic; however, most are voluntarily dismissed after the anonymous party's identity has been revealed. Current trends show federal courts are formalizing the process to issue subpoenas to determine the true identity of Internet users and courts are now applying a stricter view to protect First Amendment rights.

Keywords: Cybersmearing, Defamation, Corporations, Privacy, Regulation, ISPs.

1. Introduction

With the introduction and rapid evolution of the Internet, users have been provided an elective, often anonymous, electronic platform to globally communicate their ideas, beliefs, and commentary, whether factual or not (Sobel, 2000). The perceived anonymity of the Internet enables many users to publish messages that they otherwise might not have sent were attribution to them readily feasible (Pizzi, 2001). As the US Supreme Court explained in Reno v. American Civil Liberties Union, 521 US844, 870 (1997):

> 'through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soap box,'

with the afterthought being that the 'town crier' can remain virtually anonymous, at will. Nevertheless, with the advent of diverse forms of increasingly sophisticated electronic technology anonymity is more an illusion than a reality as anonymous message posters have come to realize that they leave behind electronic 'fingerprints' each time that they send a message (Bell, 1999). With the assistance and cooperation of Internet Service Providers (ISP's) or web-site owners, the identity of a message poster can be traced to the source computer thereby vaporizing any notion of perceived anonymity. Initially, corporations that believed themselves to have been unfairly attacked in the electronic mail medium sued ISPs claiming liability damages for having provided the mechanical platform that facilitated the distribution of allegedly defamatory information. ISPs quickly reacted arguing that they had no control over the unilateral actions of their users; and, hence, should be accorded no less legal liability protection than that enjoyed by telephone companies. The US Congress supported this position when it enacted the Communications Decency Privacy Act of 1996[1] to immunize ISPs from most defamatory liabilities[2].

The act of communicating a false, disparaging, or defamatory remark about a company, its management or stock, on the Internet has come to be referred to as 'cybersmearing' (Buckingham and Rubin, 2001). Although the term has yet to be defined by a court, it has become somewhat expansive in use, including its reference as descriptive of the process through which corporations suffer damages when a poster defames or disparages it on the Internet (Goldhaber, 2000).

Cybersmearing has caused the United States judicial system to discuss various theories and methodologies on how to balance a number of contrasting views including: the public's Constitutionally guaranteed First Amendment right to free speech and the amorphous notion of 'privacy' versus the corporation's right to protect itself from disparagement and the unauthorized distribution of proprietary information. During the last three years, cybersmearing has significantly impacted the economic conditions of hundreds of companies and thus, has resulted in a multitude of federal and state[3] court cases[4].

The first part of this paper provides a discussion of the legal issues and history surrounding cybersmearing. The second section describes key federal and state court decisions that are evolving as the foundation for cybersmear litigation. The last section provides a summary of current and evolving trends in cybersmearing cases.

2. History and Issues Surrounding Cybersmearing

Anonymity. Although the personal privacy interest in controlling the disclosure of an individual's identity is evident, often overlooked is the significance of anonymity in fostering individuality through free expression. The protection afforded by anonymity is magnified in the context of the Internet, because of the non-quantifiable number of opportunities to both publish and to receive information (Sobel, 2000). As has been noted by many, the expressive power of the Internet, although long appreciated by its users, has only recently attained constitutional status when the USSupreme Court handed down its decision in Reno v. ACLU, defining the scope of the Internet's First Amendment protection and finding:

> 'no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium' (521 US844, 870 (1997), aff'd, 929 F. Supp. 824 (E.D. Pa. 1996).

Despite the invocation of the First Amendment, anonymity cannot be considered an absolute guarantee of free expression when that expression serves to advocate damaging, illegal, or indefensible conduct. The nondisclosure of identity is often times critical for Internet message posters, particularly when engaged in discussions or postings that include topics concerning corporate financial shenanigans, marketplace deception, employment discrimination, and questionable business practices. When such messages stray into the area of criminal activity, the Electronic Communications Privacy Act ('EPCA')[5] is available to federal law enforcement authorities seeking the actual content of a communication, such as the actual text of an email message or posting. With the oversight provided by judicial scrutiny, law enforcement authorities can request the issuance of a warrant and a subpoena, if necessary, to compel ISPs to disclose

information that identifies a particular Internet user or subscriber. Heretofore, law enforcement use of the ECPA has occasionally raised Constitutional concerns regarding privacy and unlawful seizures, but such concerns have largely been muted by the impact of the September 11th terrorist attacks in the United States.

What remains, however, is serious concern regarding non-governmental, non-law enforcement access to user identity information and whether the language of the ECPA fosters such access where it provides that an ISP:

> '**may** disclose a record or information pertaining to a subscriber...to any person **other than a governmental entity**'(emphasis added) (18 U.S.C.S. 2703(c)(1)(A)).

The extent to which such disclosure threatens First Amendment privacy rights is the focus of legislative discussion in the US Congress where the Consumer Internet Privacy Protection Act of 1999 has been introduced in the US House of Representatives in an attempt to limit the distribution of personal information by an ISP (1999 H.R. 313; 106 H.R. 313).

Nevertheless, the growth of the Internet and its ubiquitous nature combined with the perceived urgency of those other than criminal investigators seeking to unmask online anonymity poses serious challenges to issues involving personal privacy and the lack of statutory protection afforded by the ECPA. Increasingly, civil lawsuits are being filed by corporations that have been the targets of critical information posted to online message boards, hosted at websites such as The Motley Fool, Yahoo! Finance, and others, seeking the identity of, and information about, anonymous Internet users. Often times financially-related websites provide readily accessible forums for the exchange of misleading, damaging, or self-serving information on publicly traded companies. Companies concerned about the dissemination of information that is considered damaging and the effects of such dissemination in the marketplace, particularly on stock prices (Keaveney, 2001), are going to court and filing lawsuits against unnamed, or 'John Doe' defendants, seeking to unmask their anonymity in order to assert damage claims allegedly resulting from anonymous postings. Disgruntled employees, dissatisfied investors, critical financial commentators, and others are potentially exposed to civil causes of action ranging from defamation and breach of contract to misappropriation of proprietary information.

The principal concerns that emerge from these corporate civil suits are the degree to which due process and matters of fundamental fairness and privacy can be compromised. Routinely, when a corporation files a civil complaint, a subpoena is served on an ISP or message board owner/ operator by plaintiff's counsel seeking the identity and related information about the anonymous online poster. The ISP may, or may not, notify their user that a subpoena has been received. When notice is provided, the user is presumably provided an opportunity to challenge the process in an attempt to quash the subpoena. The legal costs and expenses associated with such challenges, the time constraints posed by the judicial process, and the degree of success anticipated are all issues and matters that have to be carefully considered by users seeking to preserve their anonymity.

More often than not, ISPs receiving a court subpoena will simply comply as a matter of course, without any form of notice to the affected user. As a result, the user has no opportunity to quash the subpoena and the courts have no role in evaluating the propriety of the request for the identifying information sought. It is this precise absence of judicial involvement and adversarial opportunity that exposes the process of discovering the identity of anonymous users to abuse. The delicate balance between the legitimate interests and concerns of corporations seeking identifying information and the instances of potentially abusive discovery is not easily maintained; nevertheless, the risk from current legal standards that allow for lawsuits of questionable merit to be filed simply to obtain the identify of anonymous users can easily fall into the gap of unintended consequences that can stifle, deter, or eventually silence even justifiable corporate criticism.

Emerging from the hundreds of lawsuits being filed by corporate plaintiffs eager to discover the identity of anonymous Internet users is a core of legal theories that center on arguments in support of defamation, and the unauthorized use of proprietary information. This latter theory is often supplemented by claims of breach of an employment contract, whether oral or written. In defense, users have asserted arguments premised on First Amendment claims of free expression and invasion of privacy, and on notions of fundamental due process, particularly when the discovery of their identity results in an employment termination. Of equal concern is the degree to which the allegedly wrongful statements actually pose a viable cause of action. This latter is most often posed in the context of a defense to a defamation claim and the need for the plaintiff to show actual harm in order to proceed. The degree to which courts will invoke a requirement of actual harm before permitting a plaintiff to proceed on a discovery claim is currently under debate, but seems to be an evolving decisional theory that is gaining support as the result of the Dendrite International holding discussed later in this paper.

3. Key Cybersmearing Cases

ISP liability. The Reno v. American Civil Liberties Union, 521 US844 (1997), noted at the outset of this paper, was a key decision in support of exempting ISPs from vicarious liability for the actions of users; and, again as noted earlier, the US Congress codified this principle with the adoption of the Communications Decency Privacy Act of 1996[6]. However, it is important to note that neither the Reno v. ACLU nor the Communications Decency Privacy Act completely absolves the ISP from any and all liability for the actions of its users. ISPs can still be held exposed to copyright infringement liability by its users and for those types of communications deemed obscene (18 U.S.C.S. 2710). And, at least one commentator has suggested that ISPs could be held vicariously liable, even without knowledge, when either the website designer, the website owner, or the ISP (1) has the right and ability to **control**, the infringer's acts; or (2) receives a **direct financial benefit**, from the infringement (Walton, 1999). This suggestion does not really carve out any new law as both the Restatement of Torts Third and common law have both recognized the imputed knowledge concept in the context of actual and apparent agency. What is significant, though, is the fact that ISPs will have to continually develop increasingly sophisticated technologies to monitor the usage activities of users with judicial scrutiny then shifting to the adequacy of such technologies. The less adequate technologies are deemed the more likely that vicarious liability for negligence will be asserted.

Invasion of privacy based on freedom from warrantless search or seizure. United States law has long recognized the application of the Fourth Amendment to preclude warrantless searches and seizures, provided that there is neither probable cause (a criminal standard) nor areas on able expectation of privacy (a civil standard) (US. v. Katz). Absent a reasonable expectation of privacy, files stored on an Internet Service Provider's server may not be protected by the Fourth Amendment and that the consent of the ISP is all that is required for plaintiff's to have access to the identity and information of anonymous users.

In John Doe v. 2THEMART.COM Inc., 140 F. Supp. 2d 1088 (2001), the United States District Court for the Western District of Washington directly addressed the issue of the right of privacy of 'John Doe' making accusations of fraud versus the right of a corporation to protect itself from what it asserted were the defamatory implications of such statements. John Doe argued that anonymity on the Internet was a right protected by the First Amendment and that compelled disclosure of his identity was an unconstitutional invasion of his privacy. 2THEMART.COM argued that the statements were defamatory and, by definition, unprotected by the Fourth Amendment. In its decision, the court took the position that:

> 'the Internet represents a revolutionary advance in communication technology...It allows people from all over the world to exchange ideas and information freely'(at page 1101).

The court noted that the issues raised in this case challenge the scope of an individual's First Amendment rights and, thus, challenged the court to clarify the degree of proof that must first be demonstrated by the corporate plaintiff in support of its defamatory cause of action. In other words, the court was not convinced that mere allegations of defamation alone were sufficient to outweigh the defendant's right to remain anonymous. A showing that the statements made were such as to reasonably constitute defamation might first be required before disclosure would be compelled. Such reasoning would be consistent with the idea that a lawsuit must first show that it has merit before the anonymous interests of the defendant would be compromised. Of course, such reasoning presupposes that the anonymous user was first notified of the pending claim for disclosure by the ISP. Absent such notice, the argument cannot be presented. So, the question that remains is not as much one of an invasion of privacy as it is one of due process and whether an ISP should be required to provide notice of a pending subpoena in order to permit the defendant a fair opportunity to assert applicable Fourth Amendment arguments.

Courts preceding John Doe v. 2THEMART.COM had begun to explore the idea of requiring some degree of support for the merits of claims asserted before the court would compel the disclosure of anonymous user identity. In the case, In re Subpoena Deuces Tecum to America Online, Inc., 52 Va. Cir. 26 (2000) [7], a lower court in Virginia found that:

> 'the right to communicate anonymously on the Internet falls within the scope of the protections afforded by the First Amendment. [But that] the First Amendment

> [did] not absolutely protect [a defamatory statement] made anonymously nor the release of confidential inside information' (at 38).

American Online had argued that the subpoena to uncover the identity of is anonymous user should be dismissed on the basis of First Amendment concerns. However, the court held that the subpoena should stand and that any Constitutional issues, whether based on the First or the Fourth Amendments, would be more properly raised the affected party, i.e., the anonymous user and not the ISP. The court based its reasoning on the fact that the user was actually the affected party and that disclosure would ordinarily be warranted absent a showing that the subpoena would have an oppressive effect on the ISP.

The decisional structure of the In re Subpoena Deuces Tecum to America Online decision was revisited in Dendrite International, Inc. v. Does, 342 N. J. Super. 134 (2001), when a New Jersey state court was asked to issue a subpoena to Yahoo! seeking to compel disclosure of the identity of an Internet user in support of its claims of misappropriation of trade secrets, breach of contract and fiduciary duty, and defamation. In framing its decision, the Dendrite court in a lengthy opinion, made reference to a California case, Columbia Ins. Co. v. Seescandy.com, 185 F.R.D 573 (N.D. Cal. 1999), which had developed a four-prong test that a plaintiff must first satisfy before a court will compel issuance of a subpoena for identity disclosure. Interestingly, the Seescandy.com case did not center on an act of defamation; but, instead, concerned the alleged violation of a registered trademark. The plaintiff in Seescandy.com, Columbia Ins., was the assignee of various trademarks including one for 'See's Candy Shops, Inc'. The plaintiff argued that the defendant, Seescandy.com, had purposely violated the various trademark interests of the plaintiff including the misappropriation of the plaintiff's right to the 'Seescandy.com' domain name. The need for a subpoena to compel disclosure arose, because the plaintiff did not know who had registered the website name, i.e. Seescandy.com, since the site owner had used an alias when registering. The defendant, Seescandy.com, argued that there was then no law that prohibited the selection of the domain name that it chose and that a compelled disclosure of the registrant's name was unwarranted and unnecessary. The court found that since there was no apparent infringement on the trademark interests of the plaintiff there was really no need to compel disclosure of the anonymous registrant's true identity. In reaching its conclusion, the court had formulated the four-prong test, which the Dendrite court discussed and adopted.

The court in Seescandy.com held that a plaintiff seeking to unmask the author of an anonymous Internet message posting must satisfy four separate and distinct criteria before a court will compel disclosure by subpoena:

First, the plaintiff must 'identify the missing [anonymous] party with sufficient specify that the Court can determine that the defendant is a real person or entity who can be sued in federal court'(at 586).

Second, that all steps taken in the plaintiff's attempt to locate the defendant must be detailed (at 586). This is a fairly easily satisfied element as most ISP's now routinely resist disclosure of the identity of anonymous users absent some of form of compulsory process.

Third, the plaintiff must establish that its lawsuit 'could withstand a motion to dismiss' (at 586). This criteria is important since the court felt it necessary to 'prevent abuse of [the] extraordinary application of the discovery process and to ensure that [the] plaintiff has standing to pursue an action against the defendant' (at 586).

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 (at 586).

Although the court in Dendrite professed to apply the Seescandy.com four-part analysis, it actually required the plaintiff to prove a prima facie case before it would be able to obtain a subpoena to compel discovery of the identity of an anonymous user. In other words, the court felt that mere allegations of a defamatory injury were not sufficient; and, that a required element of the plaintiff's case should be actual proof of an injury to its business reputation. This principle as supported when the appellate court reviewing the lower court decision in Dendrite wrote that 'the trial court must consider and decide those applications by striking a balance between the well-established First Amendment right to speak anonymously, and the right of the plaintiff to protect its proprietary interests and reputation through assertion of recognizable claims based on actionable conduct of anonymous, fictitiously-named defendants' (Dendrite International, Inc. v. JohnDoe, No. 3, A-2774-00T3 (July11, 2001)). In effect, the Dendrite appellate decision has affirmed the requirement for a plaintiff to notify the anonymous user that they are the subject of a subpoena; and, that the plaintiff provide the actual comments inferred as defamatory, accompanied by some reasonable proof of the viability of the claims asserted.

4. Current and Evolving Trends in Cybersmearing Cases

The conflicts posed by Internet anonymity obviously require that a balance be struck between its benefits and its potential abuses. From a purely Constitutional perspective, it is evident that the balance should be heavily weighted toward the preservation of free and unimpeded online expression. As the US Supreme Court has noted:

> 'the right to remain anonymous may be abused when it shields fraudulent conduct. But...our society accords greater weight to the value of free speech than to the dangers of its misuse' (McIntyre v. Ohio Elections Commission, 514 US334 (1995)).

To date, most defendants grappling with the defense to a disclosure subpoena have asserted arguments sufficient only to resist the plaintiff and have ignored an equally fundamental alternative, namely whether or not abusive use of the discovery process by the plaintiff constitutes, in and of itself, the basis for a responsive cause of action sounding in tort. In many instances, the real purpose underlying many cybersmear suits is merely to unearth identifying information so that a corporate plaintiff can confirm its suspicions and initiate some form of non-judicial action, such as the termination of an employee suspected as the offending anonymous poster. And, once the discovery into the identity of the anonymous poster is completed, the lawsuit is quietly dropped. A number of authors and free speech advocates refer to these types of actions as 'cyber-SLAPP'

suits, the online equivalent of 'strategic lawsuits against public participation'(Gallagher, 2000). These authors maintain that such suits are not intended to vindicate valid legal claims, but instead, to invoke punitive sanctions against offenders over whom the corporate plaintiff can exert some degree of authority or control. Such punitive intent might support a tortuous claim for abuse of process against the corporate plaintiff if persuasive arguments can be crafted to credibly emphasize the vindictive intent motivating the plaintiff's discovery lawsuit. After all, if the only remedy that the plaintiff seeks to achieve is some form of non-judicial relief, such as employee termination, then how can the corporate plaintiff maintain a cause of action for disclosure alleging damage from defamatory statements that it fully intends to ultimately ignore?

Further, if employee termination is the ultimate objective of the corporate plaintiff in a cybersmear lawsuit, the manner and means of that termination may well lead to tortuous claims for wrongful termination especially if the cybersmear basis for such termination is not a clearly defined cause for termination as indicated in promulgated employment policies, procedures, handbooks, and materials. Further, selective enforcement of termination policies and procedures might additionally evidence a discriminatory intent applied through arbitrary, capricious, or subjective conduct.

Legislatively, statutory protection for the online privacy of individuals who use the Internet has been introduced in the US Senate in the form of a proposed bill entitled as the Online Personal Privacy Act (2002 S. 2001; 107 S. 2201, April 18, 2002). The bill is currently being debated in the Senate Committee on Commerce, Science, and Transportation. The bill's ultimate passage is uncertain, particularly as its language does not clearly establish standards or criteria for distinguishing civil claims having merit from those lacking merit in pursuit of remedies against anonymous posters.

5. Conclusion

In conclusion, it is clear that some measure of judicial oversight should be brought to the discovery process even when John Doe defendants are unable to retain counsel to defend their anonymity. Whether this oversight should take the form of specific requirements imposed on the corporate plaintiff or remedies extended to the aggrieved defendant is unclear. However, it is clear that all parties affected will continue to struggle with the balance of free expression and the protection of legitimate corporate interests until such time as a judicial consensus is achieved regarding the legitimacy of cybersmear claims at the outset of a corporate plaintiff's cause of action. Absent such legitimacy, the right of Constitutionally protected free expression will most likely prevail.

Notes and References

1. Pub.L. 104-104, 110 Stat. 137-139, 47 U.S.C. S. 230 provides, in relevant part, that 'no provider...of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider, 47 U.S.C.S. 230(c)(1). See also Zeran v. America Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997), holding that claims against ISP's were barred by the Communications Decency Privacy Act. Also,

Ben Ezra, Weinstein, and Company, Inc. v. America Online, Incorporated, 206 F.3d 980 (10th Cir 2000), were the court found that America Online had not acted as an information provider outside the scope of s. 230 immunity when it provided access to allegedly inaccurate information regarding Ben Ezra, Weinstein, and Company's publicly traded stock.

2. But, such immunity is not without cost, including the cost of legal fees. Moreover, such immunity does not immunize websites that link to allegedly defamatory sites; nor is immunity provided for such claims based on invasions of intellectual property or privacy rights.

3. It is interesting to note that most cybersmearing cases are filed in state court, because it is often times impossible to plead either the federal jurisdictional principle of diversity of citizenship against a defendant whose identity and residence are unknown or federal question jurisdiction where a basis for invoking any federal law is generally lacking.

4. For listings, see Cyber Securities Law Case Digest, at <http://www.cybersecuritieslaw.com> (search term:'cyber lawsuits')

5. 18 U.S.C. S. 2510 et seq. (The statute is a 1986 revision to federal wiretap laws necessitated by emerging advances in communication including the Internet.)

6.supra n1.

7. rev'd on other grounds sub. nom. America Online, Inc. v. Anonymous Publicly Traded Company, 542 S.E. 2d 377 (Va.2001).

Bibliography

(June 2001) 'CEO's E-Attack on Collection agency Brings SEC Cybersmear Suit, Sanctions', E-Business Law Bulletin 16.

(May 17, 2000) 'Creditrust Corp. Files Cybersmear Suit Against Insurer', Securities Litigation and Regulation 5.

(June 26, 2000) 'Suit Said to Be First to Smoke Out Competitor For Alleged Cybersmear', Delaware Corporate Litigation Reporter 8.

Bell, B A (1999) 'Dealing with the 'Cybersmear'', New York Journal, April 19, 1999.

Buckingham, S R and Rubin, A R (2001), 'Anonymous 'Posters' Complicate Discovery', New York Law Journal 4, November 29, 2001.

Elkin, J (2001), 'Cybersmears: The Next Generation: Advocacy Groups Seek to Protect the Identities of Company Critics', Business Law Today 42, July/August 2001.

Gallagher, M P (2000), 'In Cybersmear or CyberSLAPP Suits, Discovery Means Finding

a Defendant', New Jersey Law Journal, July 31, 2000.

Goldhader, M D (2000), 'Cybersmear Pioneer', The National Law Journal A20, July 17, 2000.

Keaveney, R (2001), The Daily Record 3A, March 9, 2001.

Pizzi, P (2001), 'Intellectual Property Grappling with 'Cybersmear' Right to Protect From Cybersmear is Balanced Against the Perceived First Amendment Rights of Anonymous Internet 'Posters' , New Jersey Law Journal, July 23, 2001.

Scheffey, T (2000), 'Unmasking Internet Bad-Mouths', The Connecticut Law Tribune, December 18, 2000.

Serres, C (2000), 'Unmasked 'Aquacool' fires back with suit', Crain's Cleveland Business 1, June 5, 2000.

Sobel, D L (2000) 'The Process that 'John Doe' is Due: Addressing the Legal Challenge to Internet Anonymity', Virginia Journal of Law and Technology, 5 Va. J.L.& Tech. 3.

Walton, T J (2000), 'Internet Privacy Law', <http://www.netatty.com/privacy/privacy.html>, (3/12/2000).