

Cybersmear: It's What The Internet Is For, Right?

Mark D. Risk
James S. Barber
Sean R. Gallagher
Julie A. Totten
Stephen E. Fox

(The authors thank Mark Mallery, Esq., for his assistance and for sharing his research and writing on the cybersmear, which was a valuable resource.)

American Bar Association
Section of Labor and Employment Law

Employment Rights and Responsibilities Committee
2005 Midwinter Meeting
Key Biscayne, Florida

March 9, 2005

I. Jurisdiction and Choice of Law Issues

Stephen E. Fox¹
Fish & Richardson, P.C.
1717 Main Street
Suite 5000
Dallas, TX 75201
214-292-9060
sfox@fr.com

(With special thanks to Natalie Arbaugh² for her valuable assistance.)

The United States Supreme Court recognized years ago that “[a]s technological progress has increased the flow of commerce between the States, the need for jurisdiction over nonresidents has undergone a similar increase.” *Hanson v. Denckle*, 357 U.S. 235, 250-51 (1958). The Court simply could not have known then where jurisdiction issues would be now - the exponential technological change in subsequent years and the advent of the Internet have no doubt given rise to a host of jurisdictional issues, among others. The jurisprudence with respect to issue of jurisdiction is, in some cases, in its infancy while, in others, it is beginning to show a pattern or direction. The answers to the many jurisdictional questions that have arisen, however, are far from easy or clear. As one commentator has observed, “[j]urisdictional issues are inherently rooted in notions of territoriality.”³ The Internet, however, transcends geographic borders, blurring, if not eradicating, the traditional notions of state and national boundaries.⁴ With the click of a button, an individual can assert his or her presence literally throughout the world – and unlike in the pre-technology era, completely anonymously. Similarly, thousands of companies have home pages on the Web through which they communicate and to which unknown individuals from around the world have instant access.

This instant worldwide access gives rise to liability of defendants in unlimited states and under unlimited laws, thereby triggering a myriad of jurisdictional questions. Among many others, those that first come to mind include: Which state’s law applies when a person lives in one state and commits an improper act over the Internet, but injures a person in another state? Does a person in one state who sends a message that affects or is read by individuals in the forty-nine

¹ Mr. Fox is a Principal in the Dallas office of Fish & Richardson P.C.

² Ms. Arbaugh is an associate in the Dallas office of Fish & Richardson P.C.

³ David A. Schulz et al., *Publishing Without Borders: Internet Jurisdictional Issues, Internet Choice of Law Issue, ISP Immunity, and On-Line Anonymous Speech*, Practising Law Institute, Patents, Copyrights, Trademarks and Literary Property Course Handbook Series, PLI Order No. G0-00MQ, (May 2, 2001).

⁴ *Id.*

other states establish minimum contacts with the others states to establish personal jurisdiction over that person? When an anonymous individual has defamed a corporation over the Internet, can the corporation establish diversity jurisdiction over that anonymous individual? Courts have only recently begun to grapple with these issues.

A. Personal Jurisdiction

One preliminary issue that may arise in establishing jurisdiction is whether the person who has engaged in cybersmear is anonymous. Rule 8 of the Federal Rules of Civil Procedure requires a “short and plain statement of the grounds upon which the court’s jurisdiction depends.” FED. R. CIV. P. 8(a)(1). It is difficult to meet this basic pleading requirement as it relates to personal jurisdiction when the defendant’s identity is unknown. In such circumstances, a subpoena addressed to the Internet service provider (discussed *supra*) to determine the individual’s identity may be the only solution for a plaintiff who wishes to sue in federal court. Because some courts have been hostile to “John Doe” lawsuits, this process may not produce significant and sustained success. However, assuming the identity of the offender does not pose this obstacle or this obstacle can be overcome, establishing personal jurisdiction by use of the Internet poses other challenges.

The issue of personal jurisdiction has been the subject of many Internet-based lawsuits in recent years and is the most developed jurisdictional issue in the Internet context. The law with respect to obtaining personal jurisdiction has long been established. But courts have struggled to apply that law in the Internet context, seeking to articulate a standard that not only embodies traditional rules, but also that accounts for new and diverse factual scenarios spawned by the Internet. While early court decisions regarding personal jurisdiction as it relates to the Internet were inconsistent, recent judicial pronouncements have begun to settle on some established principles in this area.

Under traditional principles, a U.S. District Court may assume jurisdiction over a non-resident defendant only to the extent permitted by the long-arm statute of the forum state and by the due process clause of the Fourteenth Amendment. *Int’l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945). But, perhaps unknowingly paving the way for potentially unlimited jurisdiction during the age of the Internet, the Supreme Court stated years ago that a defendant could not avoid personal jurisdiction “merely because the defendant did not physically enter the forum state.” *Burger King Corp. v. Rudzewicz*, 471 U.S. 462 (1985).

Under traditional personal-jurisdiction analysis, the defendant must have sufficient “minimum contacts” with the forum state. *Burger King Corp.*, 471 U.S. at 474; *Int’l Shoe Co.*, 326 U.S. at 316. “Minimum contacts” is defined as “some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its

laws.” *Asahi Metal Indus. Co. Ltd. v. Superior Court of California*, 480 U.S. 102, 108 (1987). Further, jurisdiction exists over a particular defendant only if its exercise “comports with traditional notions of fair play and substantial justice” or in other words, the defendant could “reasonably anticipate being haled into court” in that forum. *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980). This rule protects defendants from being forced into a foreign court to answer for their actions based on “random, fortuitous or attenuated” contacts. *Keeton v. Hustler Magazine, Inc.*, 465 U.S. 770, 774 (1984). Personal jurisdiction under this standard can arise through two avenues: (1) specific jurisdiction if it is sought within the forum in which the cause of action arose or relates to, or (2) general jurisdiction if it is not related to the cause of action. *Pinker v. Roche Holdings Ltd.*, 292 F.3d 361, 368 (3d Cir. 2002). General jurisdiction, which requires a higher level of contacts with the forum state, exists when the defendant maintains contacts within the forum that are “systemic and continuous.” *Helicopters Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408 (1984).

1. The *Zippo* Sliding Scale of Commercial Activity Test

The case that most changed the face of the jurisdictional landscape in the world of Internet litigation is *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Penn. 1997). *Zippo* applied the above traditional tests for personal jurisdiction and established a fairly straightforward sliding-scale test for determining the propriety of exerting personal jurisdiction over a non-resident defendant in the Internet context. In *Zippo*, the manufacturer of “Zippo” tobacco lighters brought an action in Pennsylvania federal district court, alleging trademark dilution, infringement, and false designation under the Lanham Act and state law against a computer news service that used domain names containing “zippo” in them. The defendant news service (“Dot Com”) was a California corporation with its principal place of business in California; it did not maintain any offices, employees or agents in Pennsylvania. Dot Com’s website contained information about the company, advertisements, and an application for its Internet news service. Dot Com’s contacts with Pennsylvania occurred almost exclusively over the Internet. *Id.* at 1121.

The *Zippo* court addressed the issue of specific personal jurisdiction because the manufacturer had conceded that general jurisdiction over Dot Com did not exist. Discussing a host of cases and commentary, the court determined that “the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet.” *Id.* at 1124. It further explained:

This sliding scale is consistent with well-developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction

that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.

Id. (internal citations omitted). In addition, the court elaborated that under traditional personal-jurisdiction principles, when an entity intentionally reaches beyond its geographical boundaries to conduct business with foreign residents, the exercise of personal jurisdiction is proper. *Id.* (citing *Burger King*, 471 U.S. at 475). Thus, the court designated three points along a continuum of commercial activity over the Internet: (1) passive, (2) interactive, and (3) “doing business over the Internet.”

In applying this sliding-scale standard to the facts of the case at hand, the court rejected arguments by Dot Com that it had merely posted information on the Web that was accessible to Pennsylvania residents, and instead categorized the case as a “doing business over the Internet” case. *Id.* at 1125. The court concluded that Dot Com had purposefully availed itself of doing business in the state, explaining that Dot Com had done more than simply advertise on the Internet in Pennsylvania and more than simply create an interactive website through which it exchanged information with Pennsylvania residents. Rather, it had contracted with approximately 3,000 individuals and seven Internet access providers in Pennsylvania, with the intended object of those transactions being the downloading of electronic messages that formed the basis of suit in Pennsylvania. Further, the court observed that,

Dot Com repeatedly and consciously chose to process Pennsylvania residents’ applications and to assign them new passwords. Dot Com knew that the result of these contracts would be the transmission of electronic messages into Pennsylvania. . . . Dot Com was under no obligation to sell its services to Pennsylvania residents. It freely chose to do so. . . . If Dot Com had not wanted to be amenable to jurisdiction in Pennsylvania, the solution would have been simple – it could have chosen not to sell its services to Pennsylvania residents.

Id. at 1126-27. In the final analysis, consistent with traditional personal-jurisdiction principles, the *Zippo* court focused on the intentional nature of Dot Com’s conduct with respect to the forum state.

The Third Circuit approved of the *Zippo* in *Toys “R” Us, Inc. v. Step Two, S.A.*, 318 F.3d 446 (3d Cir. 2003). The Third Circuit further added in *Toys “R” Us* that in deciding the personal-jurisdiction question in a cause of action arising from the defendant’s operation of a website, a court may also consider “the defendant’s related non-Internet activities as part of the ‘purposeful availment’ calculus.” *Id.* at 453 (citing *Euromarket Designs, Inc. v. Crate and Barrel Ltd.*, 96 F. Supp. 2d 824 (N.D. Ill. 2000)). The court noted that activities that may constitute the “something more” needed to establish personal jurisdiction include “contacts such as serial business trips to the forum state, telephone and fax communications directed to the forum state, purchase contracts with forum state residents, contracts that apply the law of the forum state, and advertisements in local newspapers.” *Id.* at 454-54 (citing *Barrett v. Catacombs Press*, 44 F. Supp. 2d 717, 726 (E.D. Pa. 1999)).

The clear majority of circuit courts has expressly adopted the *Zippo* test or has applied a similar analysis. For example, in *Mink v. AAAA Development LLC*, 190 F.3d 333 (5th Cir. 1999), the Fifth Circuit applied *Zippo* in a suit filed in Texas district court by the developer of a computer software program against purported competitors, alleging a conspiracy to copy the program in violation of copyright laws and patent pending rights. One of the defendant companies was a Vermont corporation with its principle place of business in Vermont. It maintained a website advertising its allegedly infringing software on the Internet. Declining to exercise personal jurisdiction, the court concluded that the defendant’s website was merely “passive”:

Essentially, [the defendant] maintains a website that posts information about its products and services. While the website provides users with a printable mail-in order form, [the defendant’s] toll-free telephone number, a mailing address and an electronic mail (“e-mail”) address, orders are not taken through [its] website. This does not classify the website as anything more than passive advertisement which is not grounds for the exercise of personal jurisdiction. This case does not fall into the spectrum of cases where a defendant clearly conducted business over the Internet nor does it fall into the middle spectrum of interactivity where the defendant and users exchange information through the Internet.

Id. at 336-37. In addition to the Fifth Circuit, the Fourth, Sixth, Eighth, Ninth and Tenth Courts of Appeals apply these principles. *See Lakin v. Prudential Sec., Inc.*, 348 F.3d 704, 710 (8th Cir. 2003) (applying the *Zippo* standard, among other factors, to determine whether general jurisdiction existed); *ALS Scan v. Digital Serv. Consultants, Inc.*, 293 F.3d 707, 713-14 (4th Cir. 2002) (expressly adopting *Zippo* in copyright infringement action and concluding that the defendant host’s website was merely passive because defendant did not select or knowingly transmit infringing photographs specifically to Maryland with the intent of engaging in business or any other transaction in Maryland”); *Neogen Corp. v. Neo Gen Screening, Inc.*, 282 F.3d

883, 889 (6th Cir. 2002) (holding that purposeful-availment requirement is met “if the web site is interactive to a degree that reveals specifically intended interaction with residents of the state”); *Soma Med. Int’l v. Standard Chartered Bank*, 196 F.3d 1292, 1299 (10th Cir. 1999) (“[W]e cannot conclude that [the defendant’s] maintenance of a passive website, merely providing information to interested viewers, constitutes the kind of purposeful availment of the benefits of doing business in Utah such that [the defendant] could expect to be haled into court in that state.”); *Cybersell, Inc. v. Cybersell, Inc.*, 130 F.3d 414, 418 (9th Cir. 1997) (holding that “something more” beyond the mere posting of a passive website was required to indicate that the defendant had “purposefully (albeit electronically) directed his activity in a substantial way to the forum state”).⁵

Some courts have noted that the *Zippo* analysis is best applied in answering the specific-jurisdiction question, as opposed to the issue of general jurisdiction. Although many courts have adopted *Zippo* in the specific-jurisdiction context, courts of appeals addressing the issue of general jurisdiction have split regarding its applicability. *Compare Gator.com Corp. v. L.L. Bean, Inc.* v. 341 F.3d 1072 (9th Cir. 2003) (applying *Zippo* and finding general jurisdiction); *Gorman v. Ameritrade holding Corp.*, 293 F.3d 506, 513 (D.C. Cir. 2002) (applying *Zippo* and finding general jurisdiction); *Somo Med.*, 196 F.3d at 1296-97 (applying *Zippo* and finding general jurisdiction) with *Revell v. Lidov*, 317 F.3d 467, 471 (5th Cir. 2002) (explaining that while it had previously adopted *Zippo*’s sliding scale, “it is not well adapted to the general jurisdiction inquiry, because even repeated contact with forum residents by a foreign defendant may not constitute the requisite substantial, continuous and systematic contact required for a finding of general jurisdiction); *Bell v. Imperial Palace Hotel/Casino, Inc.*, 200 F. Supp. 2d 1082, 1091 (E.D. Mo. 2001) (applying *Zippo* in combination with other factors).

Other courts apply *Zippo* in answering the general-jurisdiction question, but determine that it is not conclusive and/or does not apply presumptively. For example, the *Lakin*, 348 F.3d at 708, the Eighth Circuit held that the “nature and quality” of a website and determination of whether it is “interactive,” “does business” or is merely “passive,” is certainly “an important factor” in the general-jurisdiction analysis, but a variety of other factors apply depending on the circumstances. *Id.* at 711. *Lakin* explained that a website could be very interactive under *Zippo*, yet have no quantity of contacts. *Id.* at 712. In other words, the

⁵ Similarly, district courts across the country regularly apply *Zippo*. For numerous case examples segregated by categories including “passive” websites, passive websites “plus additional contact with forum state as sufficient basis for assertion of personal jurisdiction,” “direct commercial transactions over Internet in forum state as sufficient basis for assertion of personal jurisdiction, and “interactive” websites, see Richard E. Kaye, J.D., Annotation, *Internet Web Site Activities of Nonresident Person or Corporation as Conferring Personal Jurisdiction under Long-arm Statutes and Due Process Clause*, 81 A.L.R. FED. 5TH 41 (2004). See also Schulz et. al, *supra* note 1; Cindy Chen, *United States and European Union Approaches to Internet Jurisdiction and Their Impact on E-Commerce*, 25 U. PA. J. INT’L ECON. L. 423 (Spring 2004) (discussing jurisdictional issues)

contact would be continuous but not substantial, as required to establish general jurisdiction. Accordingly, the Eighth Circuit answers the general-jurisdiction question by first applying *Zippo* and, then, also looking at the quantity of the contacts within the state. *Id.* (concluding that the defendant’s website fell under the middle category of *Zippo* as an interactive website, but that the record was not fully developed to determine whether the site’s contacts with the state of Missouri were continuous and systematic).

2. *Calder* “Effects” Test

Another test courts use in the Internet context to evaluate the propriety of exercising personal jurisdiction is the *Calder* “effects” test, which has long been applied in tort cases. The test was established in *Calder v. Jones*, 465 U.S. 783 (1984), and results in the exercise of personal jurisdiction if the harm occurs in the forum state and the defendant knew that it would occur there. As illustrated by *Calder* itself, the test is particularly appropriate in cases involving defamation claims. The plaintiff in *Calder*, an entertainer who lived and worked in California, sued the National Enquirer for libel and other claims in connection with an online article written and edited by defendants in Florida and published in the National Enquirer. While the Enquirer and its distributor answered the complaint and made no objection to jurisdiction, individuals employed with the Enquirer who lived and worked in Florida challenged the exercise of personal jurisdiction over them in a California court. The Court determined that jurisdiction existed because California was the focal point both of the story and the harm suffered, explaining:

The allegedly libelous story concerned the California activities of a California resident. It impugned the professionalism of an entertainer whose television career was centered in California. The article was drawn from California sources, and the brunt of the harm, in terms of both [Plaintiff’s] emotional distress and the injury to her professional reputation, was suffered in California. In sum, California is the focal point both of the story and the harm suffered. Jurisdiction over [defendants] is therefore proper in California based on the “effects” of their Florida conduct in California. . . . [Defendants] edited an article that they knew would have a potentially devastating impact upon [the plaintiff]. And they knew that the brunt of that injury would be felt by [the plaintiff] in the State in which she lives and works and in which the National Enquirer has its largest circulation.

Id. at 789.

The *Calder* test is summarized by other courts as requiring a showing that: (1) the defendant committed an intentional act, (2) expressly aimed at the forum state, (3) causing harm that the defendant knows is likely to be suffered in the

forum state. *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 805 (9th Cir. 2004).

Some circuits regularly apply the *Calder* test to Internet cases, including in the defamation context. For example, in *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797 (9th Cir. 2004), the Ninth Circuit applied *Calder* in a defamation claim against a company that maintained a website. Arnold Schwarzenegger filed suit in California district court alleging various claims arising out of an Ohio car dealership's use of his photograph in advertisements contained in Akron-based newspapers and journals. The dealership maintained a website that could be viewed in California, but had no operations in California, no employees in California, no advertisements in California, and had never sold a car in California. The court concluded that the defendant's act -- the creation and publication of the advertisement -- was expressly aimed at Ohio rather than California and that the purpose of the advertisement was to entice Ohioans to buy or lease cars. *Id.* at 807. Further, "it may be true that [the defendant's] intentional act eventually caused harm to Schwarzenegger in California, and [the defendant] may have known that Schwarzenegger lived in California. But this does not confer jurisdiction, for [the defendant's] express aim was local." *Id.* The Fourth Circuit also regularly applies *Calder*. See, e.g., *Young v. New Haven Advocate*, 315 F.3d 256, 262 (4th Cir. 2002) (holding that Connecticut newspapers did not post materials to their websites with manifest intent of "targeting" readers in Virginia sufficient to confer personal jurisdiction over the papers in Virginia).

The *Calder* test applies only to the specific-jurisdiction question. See *Carefirst of Maryland, Inc. v. Carefirst Pregnancy Centers, Inc.*, 334 F.3d 390, 398 n.7 (4th Cir. 2003) (categorizing *Calder* as the "effects test of specific jurisdiction"). Thus unlike *Zippo*, which at least may constitute one of several factors in the analysis of general jurisdiction, *Calder* is not helpful to Internet cases giving rise to general-jurisdiction questions.

A review of the above cases reveals, however, that application of *Zippo* and *Calder* are not necessarily mutually exclusive. For example, the Fourth and Ninth Circuits use both tests, depending on the facts and circumstances of the case presented and may apply both tests to the same case. See *Carefirst of Maryland*, 334 F.3d at 398-402 (applying both tests in infringement and dilution action and concluding that organization's setting up of website did not warrant exercise of personal jurisdiction); *Panavision Int'l v. Toepfen*, 141 F.3d 1316 (9th Cir. 1998) (applying both tests and concluding that defendant was subject to specific jurisdiction in California, explaining that merely registering someone else's trademark as a domain name and posting a website was not sufficient to establish jurisdiction but that the defendant knew his conduct would have the effect of injuring the plaintiff in California).

In short, courts have unanimously held that mere presence on the Internet alone does not establish “minimum contacts” sufficient to subject a person to personal jurisdiction throughout the world. Beyond this basic rule, however, evaluation of personal jurisdiction in an Internet case will depend on the facts and circumstances of the case presented, as well as the jurisdiction in which the suit is filed. Because of *Zippo’s* advancement of the law in this area, lack of law will not be a problem.

B. Subject Matter Jurisdiction

Whether to sue in federal or state court is always a choice a plaintiff enjoys. However, in Internet-based claims, such a meaningful choice does not always exist. Because state courts maintain general jurisdiction over matters within their boundaries, filing suits against John Does in a forum of the state where the plaintiff is located or claims to have suffered injury should not pose subject-matter jurisdiction problems. On the other hand, because federal courts are of limited jurisdiction, the fact that those engaged in a cyber smear campaigns often remain anonymous may hinder a plaintiff’s ability to sue in federal court. *See Kokkonen v. Guardian Life Ins. Co.*, 511 U.S. 375, 377 (1994).

Under federal statute, federal courts may exercise jurisdiction in cases involving questions arising under federal law or in cases of diversity. 28 U.S.C. §§1331, 1332, 1367. To show diversity, the plaintiff must allege that he or she and the defendant are “citizens of different States” or “citizens of a State and citizens or subjects of a foreign state.” 28 U.S.C. §1332(a). Under the Federal Rules of Civil Procedure, a plaintiff must set forth a “short and plain statement of the grounds upon which the court’s jurisdiction depends.” FED. R. CIV. P. 8. Furthermore, there is an initial presumption that federal courts lack subject-matter jurisdiction to hear a particular suit. *Kokkonen*, 511 U.S. at 377; *Howery v. Allstate Ins. Co.*, 243 F.3d 912, 916 (5th Cir. 2001). This presumption combined with the pleading requirement would appear to make it difficult to sustain jurisdiction in federal court when the defendant’s identity and, thus, whereabouts and citizenship are unknown.

For example, in *Vail v. Doe*, 39 F. Supp. 2d 477 (D.N.J. 1999), a New Jersey resident sued a fictitious, unknown defendant, John Doe, for sending emails over the Internet that allegedly harmed the plaintiff’s reputation, causing him “upset, emotional distress, shame, humiliation and embarrassment.” To satisfy the jurisdictional requirements, the plaintiff alleged that “the statements defaming plaintiff have been sent from the State of New York. Upon information and belief, defendant John Doe is a citizen and resident of New York.” *Id.* at 477. The court began its analysis of the diversity-jurisdiction question with the rule that “[j]urisdictional statutes are to be strictly construed and the burden of proof is upon the plaintiff to affirmatively establish diversity of citizenship.” *Id.* The court refused to find that these allegations were enough to establish diversity jurisdiction, explaining that “[e]ven if the Court accepts the contention that the defamatory e-

mails are coming from New York, it does not necessarily follow that the person sending the e-mails is a resident or citizen of that state. There are many people who do not reside in New York but work in, go to school in or often visit the state.” *Id.*; see also *Hitchcock v. Woodside Literary Agency*, 15 F. Supp. 2d 246, 251 (E.D.N.Y. 1998) (dismissing complaint against John Doe defendants when the possibility that any of them existed was “purely speculative”); *Salzstein v. Bekins Van Lines, Inc.*, 747 F. Supp. 1281 (N.D. Ill. 1990) (refusing to find diversity when complaint alleged residency but was silent as to citizenship); *Bryant v. Ford Motor Co.*, 844 F.2d 602, 605 (9th Cir. 1987) (“We have repeatedly held that a suit naming Doe defendants may not be maintained in federal courts.”), *vacated after statutory amendment*, 886 F.2d 1526 (9th Cir. 1989).

On the other hand, the case law on this issue is scarce. And, some district courts have held that Doe lawsuits, which by their nature do not allege citizenship, do not destroy diversity jurisdiction. In *Macheras v. Center Art Galleries-Hawaii, Inc.*, 776 F. Supp. 1436 (D. Haw. 1991), the court allowed the plaintiff to sustain litigation in federal court against a defendant that did not allege the citizenship of the certain John Doe defendants. The court refused to follow case law standing for the proposition that the use of Doe defendants destroys diversity jurisdiction. The court warned, however, that “[a] plaintiff who names Doe defendants, files suit in federal court at his peril. If a key party turns out to be nondiverse, the action will be dismissed for lack of jurisdiction. If the statute of limitations has expired at this point, plaintiff may not be able to refile the case in state court. Plaintiff therefore bears the risk of making a mistake about the citizenship of a Doe party.” *Id.* at 1440. See also *Weber v. Kosack*, No. 96 Civ. 9581 (LMM), 1997 WL 666246, *2 (S.D.N.Y. Oct. 24, 1997) (unreported decision) (following *Macheras*).

Because the ability to establish diversity in the case of an unknown defendant is unpredictable at best, Plaintiff’s best bet when the defendant’s identity is unknown is to attempt to state a claim under federal-question jurisdiction. In Internet cases, for example, copyright infringement and trademark infringement or dilution are causes of action that are often available. See, e.g., *Zippo*, 952 F. Supp. at 1119. If the case is a straightforward defamation case with no available federal law claim, however, the plaintiff should attempt to learn the identity and citizenship of the offender through a subpoena of the Internet service provider (discussed *supra*). If all else fails, the plaintiff should just be aware that his or her likelihood of success in convincing a federal district court to hear a claim against a defendant with unknown citizenship is unpredictable and slim. In such circumstances, the plaintiff will likely have to sustain the lawsuit in state court.

C. Choice of Law

Once the personal and subject-matter jurisdiction hurdles are overcome, the next question that arises is which state’s law applies. Although Internet-based cases have dramatically increased in recent years, choice-of-law as it applies in the

Internet context has not been heavily litigated. This is perhaps because communications (and, thus defamation claims) through written articles distributed throughout several states have long been around and are not very different from Internet-based multistate communications. In Internet cases, however, courts have generally adopted the Restatement (Second) of Conflict of Laws approach to determine which jurisdiction's law should apply.⁶

All analyses of choice-of-law issues begin with Section 6 of the Restatement. Section 6 is a general choice-of-law provision providing that in all choice-of-law analyses, factors to be considered include the certainty, predictability and uniformity of result, the ease of determination and application of the law, relevant policies and interests of the states involved, the protection of justified expectation and the promotion of interstate order. RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 6.

With respect to tort claims generally, including defamation causes of action, the Restatement more specifically addresses the choice-of-law issue by looking for the jurisdiction that has “the most significant relationship” to the occurrence. RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 145. Section 145 of the Restatement states that courts should evaluate the following factors in answering this question: (a) the place of injury; (b) the place where the injury-causing conduct occurred; (c) the domicile, residence, nationality, place of incorporation and place of business of the parties; and (d) the place where the relationship, if any, between the parties is centered. *Id.*

Unlike the first Restatement, section 150 of second Restatement addresses “aggregate” or multistate communications, which includes situations when a communication is published to persons in two or more states. RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 150, cmt. a. Accordingly, this provision is particularly appropriate for cybersmear claims. Similar to Section 145, this provision states that that the law of the state with “the most significant relationship to the occurrence and the parties” applies. *Id.* It explains that under this rule, the state is usually the one in which the plaintiff is domiciled, as long as the defamatory statement was published in that state:

- (1) The rights and liabilities that arise from defamatory matter in any one edition of a book or newspaper or any one broadcast over radio or television, exhibition of a motion picture, or similar aggregate communication are determined by the local law of the state which, with respect to the particular issue, has the most significant

⁶ For a thorough discussion of choice-of-law issues and development over time, specifically as it relates to multistate defamation and the internet context, see James R. Pielemeier, *Choice of Law for Multistate Defamation – The State of Affairs as Internet Defamation Beckons*, 35 Ariz. St. L.J. 55 (Spring 2003).

relationship to the occurrence and the parties under the principles stated in § 6.

(2) When a natural person claims that he has been defamed by an aggregate communication, the state of most significant relationship will usually be the state where the person was domiciled at the time, if the matter complained of was published in that state.

(3) When a corporation, or other legal person, claims that it has been defamed by an aggregate communication, the state of most significant relationship will usually be the state where the corporation, or other legal person, had its principal place of business at the time, if the matter complained of was published in that state.

Id.

The commentary to Section 150 provides that subsections (2) and (3) should apply “unless, with respect to the particular issue, some other state has a more significant relationship to the occurrence and the parties. Whether there is such another state should be determined in light of the choice-of-law principles stated in § 6.” *Id.* cmt. b. The comment further elaborates that this will in large part depend on whether some other state has a greater interest in the determination of the particular issue than the state under subsections (2) and (3). *Id.* Further, defamation rules “are designed to protect a person’s reputation” and the selected place will usually be the place of greatest reputation harm. *Id.* cmts. e and f.

In *Wells v. Liddy*, 186 F.3d 505 (4th Cir. 1999), the Fourth Circuit, sitting in diversity, addressed the choice-of-law issue in an online defamation action and followed the Restatement approach. In *Wells*, a former secretary of the Democratic National Committee sued an individual who had advocated an alternative theory behind the Watergate break-in, implicating the secretary. The allegedly defamatory statements occurred during public appearances by the defendant and on a worldwide website. With respect to the website statements, the court followed the Second Restatement approach for multi-state defamation, and held that because the statements were published in the place of the secretary’s domicile, that state’s law applied to her defamation claim arising from these statements. *Id.* at 528-30. *See also Weyrich v. The New Republic, Inc.*, 235 F.3d 617, 254-55 (D.C. Cir. 2001) (following Restatement § 150 to apply law of place where plaintiff suffered injury by loss of his reputation); *Hitchcock*, 15 F. Supp. 2d at 251 (not expressly adopting Restatement, but describing defamation rules as “conduct-regulating” and reading New York conflicts law as requiring application of law of the place “where the tort occurred, which is the place where the plaintiff’s injuries occurred”).

II. Subpoenaing Internet Service Providers to Identify Internet Speakers

James S. Barber
Clausen Miller, PC
10 South LaSalle St.
Chicago, IL 60603-1098
312-855-1010
jbarber@clausen.com

(With special thanks to Shawn K. Jones and Jean T. Warner for their valuable assistance.)

Sean R. Gallagher
Hogan & Hartson LLP
1200 Seventeenth St., Suite 1500
Denver, CO 80202
303-454-2415
srgallagher@hhlaw.com

A. Introduction

In cyberspace, there are no editors.

“The World Wide Web exists fundamentally as a platform through which people and organizations can communicate through shared information.” *ACLU v. Reno*, 929 F. Supp. 824, 837 (E.D.Pa. 1996), *aff’d* 521 U.S. 844 (1997). It is the most comprehensive and diverse public forum ever conceived. Not only does the Internet facilitate communication on a global scale, but it also gives its users access to an heretofore unimaginable body of knowledge and diversity of opinion. The Internet has also had an enormous equalizing effect, affording individual speakers the same pulpit previously available only to political leaders, governments and large corporations. As one commentator explained, the Internet “empowers ordinary individuals with limited financial resources to ‘publish’ their views on matters of public concern.” Lyrissa Barnett Lidsky, Silencing John Doe: Defamation and Disclosure in Cyberspace, 49 *Duke L.J.* 855, 865 (2000).

The sheer number of people who use the Internet is staggering, *id.* at 831, and because of that, Congress has noted that the Internet has become a prime forum for speech. See Communications Decency Act, 47 U.S.C. § 230(a)(3). In 1998, there were approximately 47 million e-mail users in the United States. In 2003, it was projected that there would be 105 million e-mail users in the U.S. who would send over 1.5 billion e-mail messages per day, or approximately 547.5 billion e-mail messages per year. Many of these e-mail users regularly post messages on bulletin boards or in newsgroups via the Internet. And, web-based content providers such as Yahoo! host message boards on their website, and allow posters to sign up for

pseudonyms that do not require them to reveal their true identity. See Furman, *Cybersmear or Cyber-Slapp: Analyzing Defamation Suits Against Online John Does and Strategic Lawsuits Against Public Participation*, 25 Seattle U.L.Rev. 213, 217 (Summer 2001). However, those providers do track the poster's Internet Protocol addresses, known as IP addresses, allowing even anonymous posters to be identified. *Id.*

In the rough-and-tumble of Internet speech, it is not uncommon for individuals or groups to express unpopular opinions or disseminate false information. Protection afforded by supposed anonymity encourages chat room or newsgroup posters to act in ways that they otherwise may not. Because users are allowed to post messages and comments using pseudonymous names, many users believe such publication to be without consequence. Relieved of the constraints imposed by the common law, they are more free to share unfiltered opinions on a myriad of subjects, some of which would be otherwise taboo. However, the absence of checks and balances can also lead to irresponsible behavior. To be sure, the common law tort of defamation can have both a modulating and chilling effect on speech. However, whether one is posting truthful and constitutionally protected information, or attempting to defraud the investing public, no one can dispute that the Internet has made it considerably easier for one's voice to be heard by others.

In one instance, a disgruntled HealthSouth Corp. employee named Peter Krum posted anonymous messages on the Yahoo! Finance Message Board alleging that HealthSouth was on the verge of ruin, that its managers were crooked and that he was having a sexual affair with the chairman's wife. Using the name Dirk Diggler, Krum alleged that the company was a collapsing house of cards, charged that Scrushy was bilking Medicare and said he [Diggler/Krum] was having sex with Scrushy's wife. Among the things he didn't know then, Krum later admitted, was that Scrushy's wife was pregnant at the time. After bringing suit against a John Doe plaintiff and subpoenaing the ISP, HealthSouth and Scrushy were able to identify Krum. Interested readers can now find Krum's retraction on the Yahoo! Finance Message Board, in which Krum now states, "I would also like to warn others that hiding behind a fake identity and shield of anonymity does not give one poetic license and the right to embarrass others." See <http://messages.yahoo.com/bbs?action=&board=7076888&tid=hrc&sid=7076888&mid=2482>.

Faced with the obvious difficulties of identifying anonymous posters, many defamation plaintiffs opt instead to commence a defamation suit against unidentified "John Doe" defendants. Once commenced, the plaintiff issues a subpoena to a non-party Internet Service Provider ("ISP") seeking to have the ISP divulge the identity of the anonymous poster. This section addresses the propriety of that practice under Federal Rule 45, and explores some of the defenses that ISPs and posters are asserting to such actions.

B. Use of third party subpoena under Rule 45 to identify anonymous posters.

Under the Federal Rules of Civil Procedure, parties may obtain discovery of any non-privileged information relevant to the claim or defense of any party so long as the discovery appears reasonably calculated to lead to the discovery of admissible evidence. Fed. R. Civ. P. 26(b)(1). Fed. R. Civ. P. 26(b)(1) also provides that the court may order discovery of any matter “relevant to the subject matter” of the action upon a showing of good cause. This standard is “broadly and liberally construed” to permit “discovery of all facts necessary to unearth the truth.” *In re PE Corp. Sec. Litig.*, 221 F.R.D. 20, 23, 28 (D. Conn. 2003); *accord Daval Steel Prods. v. M/V Fakredine*, 951 F.2d 1357, 1367 (2d Cir. 1991) (discovery permitted where there is “any possibility that the information sought may be relevant”) (internal citation omitted). This expansive approach to discovery ensures that litigants and the Court are adequately informed of the facts in civil trials. *Hechinger Inv. Co. of DE v. Dennis Friedman Esq., et al. (In re Subpoena Issued to Dennis Friedman)*, 350 F.3d 65, 69 (2d Cir. 2003).

However, Courts have not hesitated to supervise discovery in John Doe cases, especially when they are asked to issue ex parte subpoenas to compel the identification of the anonymous posters. “District courts should not neglect their power to restrict discovery where ‘justice requires [protection for] a party or person from annoyance, embarrassment, oppression, or undue burden or expense . . .’ With this authority at hand, judges should not hesitate to exercise appropriate control over the discovery process.” *Herbert v. Lando*, 441 U.S. 153, 178-79 (1979) (Powell, J. concurring). In supervising discovery in a libel suit by a public figure, “[a] court has a duty to consider First Amendment interests as well as the private interests of the plaintiff.” *Id.* at 178.

As a general rule, discovery proceedings take place only after the defendant has been served; however, in rare cases, courts have made exceptions, permitting limited discovery to ensue after filing of the complaint to permit the plaintiff to learn the identifying facts necessary to permit service on the defendant. *Columbia Insurance Company v. Sescandy.com*, 185 F.R.D. 573, 577 (N.D. Cal. 1999). *See e.g., Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980) (finding the district court abused its discretion in dismissing the case with respect to the John Doe defendants without requiring the named defendants to answer interrogatories seeking the names and addresses of the supervisors in charge of the relevant facilities during the relevant time period); *Estate of Rosenberg by Rosenberg v. Crandell*, 56 F.3d 35, 37 (8th Cir. 1995) (permitting a suit naming fictitious parties as defendants to go forward because the allegations in the complaint were “specific enough to permit the identity of the party to be ascertained after reasonable discovery”); *Maclin v. Paulson*, 627 F.2d 83, 87 (7th Cir. 1980) (approving of fictitious name pleadings until such time as the identity of the plaintiffs “can be learned through discovery or through the aid of the trial court”). In the even rarer case, a district court has *sua sponte* issued an order directing revelation of facts necessary to determine the true

name of a John Doe defendant. *See Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 390 n. 2, 91 S.Ct. 1999, 29 L.Ed.2d 619 (1971) (noting that the trial court had ordered the United States attorney to identify "those federal agents who it is indicated by the records of the United States Attorney participated in the . . . arrest of the [petitioner]") (quoting the district court's order). In the Ninth Circuit such exceptions to the general rule are generally disfavored. *See Gillespie*, 629 F.2d at 642. However, even in that circuit, a district court does have jurisdiction to determine the facts relevant to whether or not it has *in personam* jurisdiction in a given case. *See Wells Fargo & Co. v. Wells Fargo Express Co.*, 556 F.2d 406, 430 n. 24 (9th Cir. 1977).

1. Liability of Internet Service Providers for Statements Published by Others on their Website and the Impact of the Communications Decency Act.

At common law, one who repeats or republishes a defamatory statement made by another generally was as liable for the publication as the publication's author. The English rule was that every sale or delivery of each single copy of a newspaper or circular was a distinct publication, thus giving rise to a separate claim for defamation. See Prosser and Keeton on *Torts*, 5th Edition, p. 800 (1984). Every repetition of the defamation was held to be a publication in itself, even though the repeater stated the source or made clear that he did not believe the imputation. *Id.*, p. 799 (1984). As the law of defamation developed, courts held that to be liable, the defendant must be the "publisher" of the allegedly defamatory material, that is, one who has some involvement in the creation of the content. These "publishers" were contrasted with "distributors" such as bookstores and "common carriers" such as telephone companies. Liability only attaches for the latter if they know, or have some reason to know, prior to the distribution, that the content is defamatory. See Babcock, et al., Publishing Without Borders: Internet Jurisdictional Issues, Internet Choice of Law Issue, ISP Immunity, and On-Line Anonymous Speech, 651 PLI/Pat 9 (May 2, 2001).

ISPs provide two basic services to their clients: access and presence. Access services consist of an account through which the client can access the Internet and send e-mail. A presence account generally includes hard drive space that permits the client to have a web page or file transfer site. This latter service, known as domain hosting, allows individuals and entities to rent storage capacity and web site services from a service provider. See *Columbia Insurance Company v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

Prior to enactment of the Communication Decency Act, 47 U.S.C. § 230, courts that confronted the issue of whether an ISP is liable for statements published on the ISP's website, not surprisingly, reached varying results. In *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991), the court held that under New York law the computer service company was a distributor, not a publisher, for purposes of tort liability. Thus, under new York law, the computer service company

CompuServe could not be held liable for allegedly defamatory statements. However, in *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063-94, 1995 WL 323710, 23 Media L. Rep. (BNA) 1794 (N.Y. Sup. May 24, 1995), a court held that the computer service company Prodigy was a publisher, not a distributor, for purposes of defamation claims. The Stratton Oakmont court noted that, unlike CompuServe, “Prodigy held itself out to the public and its members as controlling the content of its computer bulletin boards” and “actively utilize[d] technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and ‘bad taste.’” *Id.* at 4. This was deemed to constitute editorial control and Prodigy was found to be “a publisher not a distributor.” *Id.*

The impact of ISP litigation was not lost on Congress. Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium, and “[t]he imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech.” *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997). Recognizing that the Internet had flourished, to the benefit of all, with a minimum of government regulation, and acting to preserve the “vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation,” Congress enacted The Communications Decency Act of 1996, Pub. L. No. 104-104 § 502(e), 110 Stat. 56, 133 (codified as amended in scattered sections of 18 and 47 U.S.C.) (“CDA”). The purpose of the CDA, the Fourth Circuit has observed, is “to maintain the robust nature of Internet communication and accordingly, to keep government interference in the medium to a minimum.” *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997).

The CDA provides in pertinent part:

(1) No provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider. . . .

(2) No provider or user of an interactive computer service shall be held liable on account of –

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

47 U.S.C. § 230(c).

Thus, under § 230 of the CDA, interactive service providers and users cannot be held liable for the republication or redistribution of statements "provided by any other content provider." 47 U.S.C. § 230(c)(1). An "interactive computer service" is broadly defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server. . . ." 47 U.S.C. § 230(f)(2). Courts construing § 230(f)(2) have recognized that the definition includes a wide range of cyberspace services, not only Internet service providers. See *Optinrealbig.com, LLC v. Ironport Systems, Inc.*, 323 F.Supp.2d 1037 (N.D.Cal. 2004); see, also, *Blumenthal v. Drudge*, 992 F.Supp. 44 (D.D.C. 1998) (AOL is an "interactive computer service"); *Gentry v. eBay, Inc.*, 99 Cal.App.4th 816, 831 & n. 7, 121 Cal.Rptr.2d 703 (2002) (on-line auction website is an "interactive computer service"); *Schneider v. Amazon.com*, 108 Wash.App. 454, 31 P.3d 37, 40-41 (2001) (on-line bookstore Amazon.com is an "interactive computer service").

The majority of federal and state courts that have addressed the scope of section 230 have concluded that that section 230(c)(1) creates a federal immunity to any state-law cause of action that would make an interactive computer service liable for information originating with a third party. These courts have held that "[c]laims seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions--such as deciding whether to publish, withdraw, postpone or alter content--are barred." *Carafano v. Metrosplash.com, Inc.*, 207 F.Supp.2d 1055, 1064 (C.D.Cal. 2002). See, e.g. *Green v. America Online*, 318 F.3d 465 (3rd Cir. 2003); *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997); *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003); *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003); *Ben Ezra, Weinstein & Co., Inc. v. America Online, Inc.*, 206 F.3d 980 (10th Cir. 2000); *Doe v. America Online, Inc.*, 783 So.2d 1010 (Fla. 2001).

In contrast, courts have held that where a service provider contributes to the content, it is not immune under the CDA. See generally, *Optinrealbig.com, LLC v. Ironport Systems, Inc.* For example, in *Carafano v. Metrosplash.com*, 207 F.Supp.2d 1055 (C.D.Cal. 2002), the defendant provided multiple-choice questions and a series of essay questions that shaped the eventual content that subscribers posted. This rendered the defendant "responsible . . . in part for the creation or development of information provided through the Internet. . . ." *Id.* at 1066-1067. Similarly, in *MCW, Inc. v. Badbusinessbureau.com*, 2004 WL 833595 (N.D.Tex.). April 19, 2004), the defendants operated a web site that served in part as a consumer complaint forum. Not only did the defendants post consumer complaints, they organized them geographically by company and under various other headings including "Con Artists" and "Corrupt Companies." *Id.* at 9 fn. 10. Moreover, the defendants contributed to the content by instructing a consumer to take photos to include in his complaint that defendants then posted. *Id.* at 10. Thus, the

defendants did not merely exercise the traditional rights of a publisher, they contributed to and shaped the content. Accordingly, they were not immune from liability. *Id.*

2. Use of John Doe Complaints to Obtain Identity of Anonymous Speaker.

The first step taken in prosecution of a defamation action against an anonymous speaker is usually the filing of a lawsuit against one or more “John Doe” defendants. Here, litigants quickly find that advances in technology have far outpaced advances in litigation rules. The Federal Rules of Civil Procedure do not expressly provide for anonymous pleading, although the Supreme Court has long allowed plaintiffs to bring actions using pseudonyms to preserve anonymity. The situation is somewhat more complicated, however, when the action is brought against an anonymous defendant. For example, Rule 4 of the Federal Rules expressly requires that a civil plaintiff serve a civil defendant with a copy of the summons and complaint within 120 days of filing the lawsuit. F.R.Civ.P. 4(m). Nonetheless, federal courts will grant some leeway in situations involving John Doe suits, often allowing limited discovery directed at identifying the defendant. See Furman, *Cybersmear or Cyber-Slapp: Analyzing Defamation Suits Against Online John Does and Strategic Lawsuits Against Public Participation*, 25 Seattle U.L.Rev. 213, 217 (Summer 2001).

Some states have statutes that permit civil actions against unknown persons. Under Illinois law, for example, a suit involving an unknown party may proceed so long as the complaint acknowledges unknown parties, steps have been taken to find said parties, and notice has been given to these parties by publication. See *Chandler v. Ward*, 58 N.E. 919, 924 (Ill. 1900) (defining necessary parties as those connected with the subject matter in question). See generally Sunkel, *And The I(SP)s Have It . . . But How Does One Get It? Examining The Lack of Standards for Ruling on Subpoenas Seeking to Reveal the Identity of Anonymous Internet Users in Claims of Online Defamation*, 81 N.C.L.Rev. 1189, 1198 (March 2003).

The inability to identify the defendant can also make it difficult for the plaintiff to properly plead its complaint. Some states require the plaintiff to describe the unknown defendant sufficiently to ensure that they are a legally accountable person or entity. See *People v. Seda*, 712 N.E.2d 682, 684 (N.Y. 1999) (holding the statute of limitations was tolled in a case where the state did not know the identity of the defendant, and referred to him merely as the “Zodiak killer”). Similarly, some courts require the plaintiff to prove that the identity of the defendant is, in fact, unascertainable through the exercise of due diligence. *Reed v. Gregory*, 46 Miss. 740, 741-42 (1872) (explaining that, while the recently enacted state statute authorized notice by publication as a sufficient means of notice for unknown heirs in a chancery suit to divide the estate, such publication is only sufficient if the plaintiff first diligently attempts to ascertain the identity of the unknown, interested parties). Moreover, the plaintiff may have to prove that he is,

in good faith, pursuing claims against the unknown parties in a timely manner, *Martin v. McCabe*, 213 S.W.2d 497, 503 (Mo. 1948) (holding that if the defendant was unnamed merely due to a lack of reasonable inquiry by the defendant, judgment against the defendant is vitiated); *Berry v. Howard*, 146 N.W. 577, 580 (S.D. 1914) (holding that plaintiff did not exercise due diligence in discovering the identity of the unknown heirs and, therefore, notice to them by publication did not serve as reasonable notice) and that he is not stalling to create new theories of liability. Finally, the plaintiff must attest, by affidavit, that he has met all of these requirements. *Berry*, 146 N.W. at 580. Document1zzFN_F71” See generally Sunkel, *And The I(SP)s Have It . . . But How Does One Get It? Examining The Lack of Standards for Ruling on Subpoenas Seeking to Reveal the Identity of Anonymous Internet Users in Claims of Online Defamation*, 81 N.C.L.Rev. 1189, 1198 (March 2003).

In addition, it may be impossible to establish the requisite subject matter jurisdiction for suits in federal court when one is unable to comply with rule 8(a)'s requirement that a complaint set forth “a short and plain statement of the grounds upon which the court’s jurisdiction depends. . . .” Some courts refuse to hear John Doe cases. See *Salzstein v. Bekins Van Lines, Inc.*, 747 F. Supp. 1281, 1283 (N.D. Ill. 1990) (noting the court's disfavor of diversity jurisdiction in Doe defendant cases), *Macheras v. Center Art Galleries-Hawaii, Inc.*, 776 F. Supp. 1436, 1440 (D. Hawi'i. 1991) (“A plaintiff who names Doe defendants, files suit in federal court at his peril.”); see also *Weber v. Kosack*, 96 Civ. 9581 (LMM), 1997 U.S. Dist. LEXIS 16786 at 7-9 (S.D.N.Y. Oct. 24, 1997) (discussing the struggle that federal courts face in determining whether unknown parties meet the requirement of diversity jurisdiction and denying defendant's motion to dismiss the case for lack of subject matter jurisdiction). But see *Dunn v. Paducah Int'l Raceway*, 599 F. Supp 612, 613 n.1 (W.D. Ky. 1984) (determining that a Doe defendant does not destroy good faith allegations of diversity of citizenship). In addition, Congress has passed a statute declaring that the citizenship of anonymous defendants should be ignored for removal purposes. Judicial Improvements and Access to Justice Act, Pub. L. No. 100- 702, § 1016(a), 102 Stat. 4642, 4669 (1988) (codified at 28 U.S.C. § 1441(n) (2000)). Commentary to the rule suggests that if the identity of the defendant is later found to destroy diversity, the court should act (under 28 U.S.C. § 1447(e) (2000)) to either deny joinder or permit joinder and remand the case back to the appropriate state court. H.R. Rep. No. 100-889, at 71 (1988), reprinted in 1988 U.S.C.C.A.N. 6031, 6031-32. See generally Sunkel, *And The I(SP)s Have It . . . But How Does One Get It? Examining The Lack of Standards for Ruling on Subpoenas Seeking to Reveal the Identity of Anonymous Internet Users in Claims of Online Defamation*, 81 N.C.L.Rev. 1189, 1198 (March 2003).

ISP may respond to such a subpoena by notifying the poster that his identity is being sought. ISP policies vary in this regard. For example, Comcast’s policy states that,

“We make every reasonable effort to protect subscriber privacy as described in this Policy. Nevertheless, we may be required by law to disclose personally identifiable information about a subscriber without his or her consent and without notice in order to comply with a valid legal process such as a subpoena, court order, or search warrant. We may also use or disclose personally identifiable information about you without your consent to protect our customers, employees, or property, in emergency situations, to enforce our rights in court or elsewhere, or directly with you, and for violations of the Service's terms of service and policies (including our Acceptable Use Policy).”

Comcast.net Privacy Statement, available at <http://www.comcast.net/privacy/#disclosure>. See also, Cable TV Privacy Act of 1984, 47 USC Sec. 551(b)(2). Similarly, Yahoo!'s privacy policy provides that the company

“respond[s] to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims” and believes that “it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo!'s terms of use, or as otherwise required by law.”

Yahoo.com Privacy Policy, available at <http://privacy.yahoo.com/privacy/us/>.

3. First Amendment Protection for Anonymous Speech

a. Free Speech and the Internet

The United States Supreme Court in *Reno v. American Civil Liberties Union, et al.*, 521 U.S. 844 (1997) held that First Amendment protections apply to the Internet. The court reasoned that the invasive nature of other broadcast medium, such as the radio and television, which gave rise to a need for some regulation of speech does not exist in the Internet media and therefore regulation is tolerated to a lesser degree. Instead, the Supreme Court looks at the Internet a more comparable to “a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.” 521 U.S. at 849-50. As a result, the Supreme Court concluded that First Amendment Protections extend to speech on the Internet. *Id.* at 885. Moreover, the Court itself drew the analogy between the anonymous speech cases of *Talley* and *McIntyre* by stating, that an internet poster, “[t]hrough the use of Web pages, mail exploders, and newsgroups, can become a pamphleteer.” 521 U.S. at 869.

b. The First Amendment and Anonymous Speech

One defense often raised in defamation cases arising out of anonymous bulletin board postings is that such anonymous speech is protected under the First Amendment. The Supreme Court has held that the right to anonymity is more than

just one form of protected speech; it is part of “our national heritage and tradition.” *Watchtower Bible & Tract Soc’y of New York, Inc. v. Village of Stratton*, 536 U.S. 150, 166 (2002). Relying specifically on the Supreme Court decision in *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), defendants often argue that anonymous postings on the Internet are akin to political speech that is “not [a] pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent.” *McIntyre*, 514 U.S. at 342. *McIntyre* involved an Ohio election law that prohibited the distribution of anonymous campaign literature. Relying on a 1960 Supreme Court decision, *Talley v. California*, 362 U.S. 60 (1960) extending the freedom to publish anonymously to the advocacy of political causes, *McIntyre* argued that the Ohio regulation violated the First Amendment. In analyzing the application of the Ohio regulation, the Court in *McIntyre* first noted that the statute at issue burdened “core political speech” and that the subject regulation was content-based. Thus, the Court applied the strictest level of scrutiny to the regulation, requiring that the government demonstrate that the rule is narrowly tailored to serve an overriding state interest. Noting that an author’s name and address contribute little to a reader’s ability to evaluate the message, the Court concluded that Ohio failed to demonstrate that its interests justified a prohibition of all anonymous election-related speech.

Several courts have addressed whether and under what circumstances subpoenas on ISPs would be enforced. In *Columbia Insurance Company v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999) (“Seescandy”), a subpoena sought the identity of the defendant, an alleged trademark infringer. The court ruled that the party seeking the subpoena needed to satisfy certain standards of proof at a prediscovery hearing, explaining that:

This ability to speak one’s mind without the burden of the other party knowing all the facts about one’s identity can foster open communication and robust debate. Furthermore, it permits persons to obtain information relevant to a sensitive or intimate condition without fear of embarrassment. People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court’s order to discover their identity. Thus some limiting principles should apply to the determination of whether discovery to uncover the identity of a defendant is warranted.

Id., at 578. See also *Doe v. 2theMart.com*, 140 F.Supp.2d 1088, 1093 (W.D. Wash. 2001) (“if Internet users could be stripped of . . . anonymity by a civil subpoena enforced under liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment Rights.”); *Dendrite v. Doe*, 775 A.2d 756, 771 (N.J. App. 2001) (strict procedural safeguards must be imposed “as a means of ensuring that plaintiffs do not use discovery procedures to ascertain the identities of unknown defendants in order to harass,

intimidate or silence critics in the public forum opportunities presented by the Internet.”)

The court in the *Seescandy* decision set out four factors to be considered in determining whether such discovery should be granted:

- (1) The plaintiff should identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court;
- (2) the party should identify all previous steps taken to locate the elusive defendant, to ensure that plaintiffs make a good faith effort to comply with the requirements of service of process and specifically identifying defendants;
- (3) the plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss; and
- (4) the plaintiff should file a request for discovery with the Court, along with a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible.

185 F.R.D. at 578-580.

4. How Courts Are Ruling On These Issues

a. Information Can Be Too Public, When A Company Is Too Public.

In *Global Telemedia Int'l, Inc. v. Does 1-35*, 132 F. Supp. 2d 1261 (N.D. Cal. 2001), the court applied California's unique anti-SLAPP statute, which protects anonymity when speaking about a public concern.⁷ The plaintiff asserted claims of trade libel, libel per se, interference with contractual relationships and prospective economic advantage against several posters on an Internet chat room. Then, the plaintiff requested expedited discovery and subpoenas to uncover the identity of the posters. The posters filed motions to strike pursuant to the anti-SLAPP statute. The plaintiff was a publicly traded company and, therefore, the court determined there was a public issue under the state's anti-SLAPP statute. However, the court observed that the defendants were exercising free speech rights by stating opinions about a matter of public concern -- market fluctuations. As a result, the court

⁷ Cal. Code Civ. Proc. § 425.16 was introduced by California legislators in direct opposition to Strategic Litigation Against Public Participation (SLAPP) Lawsuits. The statute allows a defendant to dismiss a lawsuit if the alleged bad act arose from his/her exercise of free speech on an issue of public concern and there is no probability of success on the claims.

found that the plaintiff had little probability of success in the suit and the subpoena was stricken.

b. Proving The Compelling Interest in Protecting Company Outweighs First Amendment Rights

Two primary tests have developed to aid a court in balancing the plaintiff's right to seek justice from a tortfeasor and the accused tortfeasor's right to anonymous speech. The first was presented in *Columbia Insurance Co. v. Seescandy.com*, discussed *supra*, which focuses on limiting overbroad discovery requests and a good faith basis for seeking the discovery. The second, and increasingly more accepted, was first presented in *Dendrite International, Inc. v. Doe, No. 3*, discussed *infra*, which strikes the balance between a good faith pursuit of a claim and the required First Amendment balancing.

c. A Subpoena Must Be Centrally Needed to Advance the Claim.

In a seminal case, *In re Subpoena Duces Tecum to America Online*, No. (Misc. Law) 40570, 2000 V. Cir. LEXIS 220 (2000), a publicly traded company sought to learn the identities of AOL subscribers in order to name them as defendants in a lawsuit in order to stop defamation and disclosure of confidential information. When served with subpoena, AOL refused to disclose the names of the cybersmearers. The Virginia court, recognizing the First Amendment right of Internet anonymity, held that AOL could assert the First Amendment rights of its users. However, the trial court still ruled against AOL allowing the plaintiff to move forward with discovery, and AOL appealed. On appeal, the court first held that an ISP could assert the First Amendment rights on behalf of its subscribers. *Id.* at *5-6. Then, to determine whether to enforce the subpoena to reveal a user's identity, the court established a two-part test. Under this two part test, the plaintiff must show proof, satisfied by the pleading or evidence that:

- (1) There is a "a legitimate, good faith basis" that the plaintiff may be the victim of conduct actionable in that jurisdiction;
- (2) "[T]he subpoenaed identity information [is] centrally needed to advance that claim."

Id. at *8. Applying this two part test, the court allowed identification of the anonymous users. The court reasoned, that there is a "compelling state interest to protect companies operating within its border from [dissemination of trade secrets and defamation]....Those who suffer damages as a result of tortious or other actionable communications on the Internet should be able to seek appropriate redress by preventing the wrongdoers from hiding behind an illusory shield of purported First Amendment rights." *Id.* at 35,*36.

d. Subpoenaing Non-parties, Beyond Seescandy.com.

Doe v. 2TheMart.com Inc., 140 F.Supp.2d 1088, 1094-95 (W.D. Wash. 2001) involved a company which was a defendant in a shareholder derivative action in California. As an affirmative defense to the derivative action, the company alleged that anonymous, nonparty, Internet posters had posted statements on the Internet to allegedly cause a dip in the Company's stock price. The plaintiff sought a subpoena for disclosure of an anonymous Internet poster from the ISP.

The trial court issued the subpoena and the company then served the subpoena on the ISP in Washington. The ISP notified the Internet users, after which one of the Internet users filed a motion to quash in a District Court in Washington. The District Court determined that "the standard for disclosing the identity of a non-party witness must be higher than that articulated in *Seescandy.com* and [*In re America Online*]." *Id.* at 1094. Disclosure of a non-party is: "only appropriate in the exceptional case where the compelling need for the discovery sought outweighs the First Amendment rights of the anonymous speaker." *Id.* In lieu of the *Seescandy* standard, the court adopted the following, four-part standard for revealing the anonymity of a non-party:

The 2TheMart.com Test

- (1.) **Good Faith:** The subpoena seeking the information must be issued in good faith and not for any improper purpose;
- (2.) **Core Claim:** The information sought must relate to a core claim or defense;
- (3.) **Direct Relevance:** The identifying information must be directly and materially relevant to that claim or defense; and,
- (4.) **Sole Available Source:** Information sufficient to establish, or to disprove, that claim or defense cannot be obtained from any other source. *Id.*

Based on the evidence presented, the court found that the information sought did not relate to the core defense of the company, nor was the identity of the Internet users directly and materially relevant to the company's defense in the derivative action. Accordingly, the court denied the subpoena.

e. Can a Plaintiff-Company Remain Anonymous While Seeking the Identity of its Cybersmearer?

In *America Online, Inc. v. Anonymous Publicly Traded Co.*, 542 S.E.2d 377 (Va. 2001), the Court did not focus on whether the smearer could remain anonymous. Rather, the Court adjudicated whether the plaintiff may remain anonymous. In pursuing its claims the plaintiff, a publicly traded company, sought to remain anonymous while trying to obtain subpoenas against anonymous online

users. The plaintiff argued that it had to remain anonymous “because disclosure of its true company name will cause irreparable harm.” 542 S.E.2d at 380. The lower court allowed the plaintiff to proceed anonymously and the ISP, AOL, appealed. On review, the Virginia Supreme Court noted that generally the test for permitting a plaintiff to proceed anonymously is “whether the plaintiff has a substantial privacy right which outweighs the customary and constitutionally-embedded presumption of openness in judicial proceedings.” 542 S.E.2d at 363-64. Noting that fear of “suffering some embarrassment or economic harm is not enough,” the Court reasoned that the plaintiff had not borne its burden of showing of reasonable concern over potential economic harm. 542 S.E.2d at 384. The Court then reversed the lower court’s order and held that the plaintiff could not proceed anonymously.

f. **The Key to Success: Establishing An Employer/Employee Relationship To Over-Come Anonymity**

Three factual issues greatly increase an employer’s chance of success in pursuing the identity of a cybersmearer. These three factors are as follows: (1) the defendant was at one time an employee; (2) employees executed some form of confidentially agreement; (3) that the posted statements provide evidence of a breach thereof. *Immunomedics v. Jean Doe*, 775 A.2d 773, 775 (NJ Ct. App. 2001); *see also, Dendrite International, Inc. v. Doe, No. 3*, 775 A.2d 756 (NJ Ct. App. 2001)(upholding discovery request when it related to two individuals who were clearly employees); *ViroLogic, Inc. v. Doe*, No. A101571 & A102811, 2004 Cal. App. Unpub. LEXIS 8070 (Cal. Sept. 1, 2004) (when posting indicated access to confidential inside information and when discovery established speaker was a contractor who had signed a confidentiality agreement, disclosure of speaker’s identify was proper). These cases and their factors are discussed in further detail below and provide the road map to the easiest way to obtain expedited discovery.

1. **Tests and More Tests: Adding the First Amendment to the Test.**

In the *Dendrite* case, a corporation, filed suit against four fictitiously named defendants. *Dendrite International, Inc. v. Doe, No. 3*, 775 A.2d 756 (NJ Ct. App. 2001). The company claimed breach of employee or confidentiality agreements, as well as, breach of fiduciary duty, misappropriation of trade secrets, interference with a prospective business advantage, defamation and a variety of other causes of action. Two of the unnamed individuals were identified as having been employed by the company at some point in time. The trial court permitted discovery pertaining to the identity of those two individuals.

However, the trial court denied discovery regarding the identity of two other individuals, who had no employment relationship with Dendrite. Dendrite appealed the trial court’s decision. The Court of Appeals affirmed the lower court’s decision denying discovery against the non-employee. The court reasoned that the

claim would not stand against the First Amendment protections because the plaintiff could not establish harm, an essential element of a defamation claim.

The court's decision in *Dendrite* court established a **four-prong test** for determining whether to compel an ISP to disclose the identity of anonymous users.

Four Prong Test:

- (1) **Efforts to Notify:** The plaintiff must show: (a) efforts to notify the cybersmearers "that they are the subject of a subpoena," and (b) allow time for the cybersmearer to file and serve opposition to the application prior to filing the action. *Dendrite*, 775 A.2d. at 760.

Practice Tip: "[N]otification efforts should include posting a message of notification, of the identity discovery request, to the anonymous user on the ISP's pertinent message board." *Id.*

- (2) **Specificity:** "[I]dentify and set forth the *exact statements* purportedly made by *each* anonymous poster that plaintiff alleges constitute actionable speech." *Id.* (*emphasis added*)
- (3) **Adequacy of Case:** "[T]he complaint and all information provided to the court should be carefully reviewed to determine whether plaintiff has set forth a *prima facie* cause of action against the fictitiously-named anonymous defendants," with sufficient evidence for each cause of action. *Id.* This test also requires a showing that plaintiff's action can withstand a motion to dismiss for failure to state a claim upon which relief can be granted. *Id.*
- (4) **First Amendment Balancing:** The final prong of the *Dendrite* test is a balancing of "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." *Id.* at 760-61 (*emphasis added*).

The *Dendrite* test places a heavy -- but not insurmountable -- burden on employers seeking a subpoena for cybersmear.

2. Further Refining the Pursuit of Discovery: *Immunomedics v. Doe*, 775 A.2d 773 (NJ App. Ct. 2001).

In *Immunomedics v. Doe*, 775 A.2d 773 (NJ App. Ct. 2001), the plaintiff alleged that the defendant had posted a message containing confidential and proprietary information about the company on a Yahoo! finance bulletin board. The trial court denied the anonymous defendant's motion to quash a subpoena *duces tecum* issued to Yahoo!, and the defendant appealed. On appeal, the Court noted that the plaintiff had relied a message posted by the defendant describing herself as "[a] worried employee." Therefore, the court found that the plaintiff had presented (1) *prima facie* proof that the Cybersmearer was an employee. Further, the plaintiff was able to supply evidence, (2) that all employees executed a confidentially agreement, (3) and, that the posted messages provided evidence of a breach thereof. Moreover, the confidentiality agreement contained a choice of law provision, which stated the laws of New Jersey were applicable, and therefore the court concluded it had jurisdiction. (4) Using the guidelines set forth in *Dendrite*, the *Immunomedics* court concluded that, in balancing the anonymous free speech rights against the strength of the *prima facie* case presented, disclosure was proper. *Id.* The court reasoned, "[i]ndividuals 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." *Id.* at 777-78.

The *Immunomedics* decision shows that the likelihood of success can be increased based on the cause of action pursued. The plaintiff in *Immunomedics* based its causes of action on a violation of a confidentiality agreement and handbook, and a breach of the common law duty of loyalty -- not defamation as in *Dendrite*. *Id.* The court in *Immunomedics* noted this difference, specifying that the plaintiff in *Dendrite* failed because it could not demonstrate damages, but in *Immunomedics* the plaintiff could prove the necessary elements of breach of a contract.

Practice Tips for Confidentiality Agreements:

Practice tips can be draw from the reasoning of the *Immunomedics* court regarding what to include in an employer's confidentiality agreement.

The agreement should acknowledged that:

- 1) the employee agrees to waive the right to speak against the company, including public or private disclosures while using the intranet/ internet;

- 2) the employee submits to the jurisdiction of the laws of the state of incorporation of the company;
- 3) the employee consents to providing his or her name if requested in any subpoena enforcement action;
- 4) the agreement will survive the employment of the employee.

g. Continuing the Application of Precedent- More Practice Tips.

In *ViroLogic, Inc. v. Doe*, No. A101571, A102811, 2004 Cal. App. Unpub. LEXIS 8070 (2004) a company asserted claims after an anonymous person (Doe) posted inflammatory messages on an Internet bulletin board. The publicly traded company then filed suit for misappropriation of trade secrets, defamation, trade libel, unfair competition and intentional interference with prospective economic advantage. ViroLogic did not identify any allegedly actionable statements, and sought to discover the identity of the poster. ViroLogic sought permission to pursue expedited discovery from Yahoo! regarding the identity of the anonymous posters, limiting its claims for purposes of the motion to misappropriation of trade secrets. ViroLogic also filed, under seal, records of, “internal, as yet nonpublic financial information” allegedly disclosed by Doe. One such record filed with the court regarded the activities ViroLogic undertook in pursuing a potential business partnership. Overnight, the court-filed records started appearing on the Yahoo! message board.

As a result, the trial court allowed limited discovery and a deposition of Doe. However, the court only allowed outside counsel to attend, not the company’s inside counsel. Once outside counsel discovered Doe was a contractor of ViroLogic, they filed a motion to disclose the information to certain executives at ViroLogic.

Counsel argued that they needed to disclose Doe’s employment status to corporate officers in order to develop a *prima facie* case in opposition to Doe’s motion to strike. Doe’s employment relationship would be helpful, they argued, because Doe worked for a brief period as a consultant and had signed an agreement prohibiting disclosure of confidential and trade secret information. Moreover, ViroLogic’s attorneys pointed out that Doe held a substantial number of shares of ViroLogic stock and was closely related to a current ViroLogic employee.

The trial court denied the request of ViroLogic’s outside counsel to disclose Doe’s identity to the company and in-house counsel. The court also granted Doe’s special motion to strike ViroLogic’s complaint under California’s anti-SLAPP statute. On review, the Appellate Court overturned the lower court. In doing so, the Appellate Court noted three things: (1)ViroLogic had set forth sufficient details in its motion seeking Doe’s identity and therefore the trial court should have been

on notice that other claims were contemplated that needed investigation; (2) Regarding the trade secret claim, the timing of the leak evinced a likelihood that the information was disclosed breaking a confidentiality within the company; and (3) Doe's contact was only one of a few people who would receive the inside information was enough to move forward.

Therefore, the court concluded that, although, the evidence present may not have risen to the level of trade secret, it provided a good faith basis to believe the company may have some legally valid claims against Doe for disclosure of confidential information. Therefore, the court ruled that the evidence presented was sufficient to support a motion for disclosure.

From the *ViroLogic* opinion the following strategies can be gleaned:

ViroLogic Practice Tips:

Plaintiff/Employer Strategy- Creating a Defense to a Motion to Strike a Subpoena Request.

It is helpful if you can assert that:

- (a) **Access:** It is imperative to consult with your client to learn more about Doe and his/her access to confidential information, either directly or through others
- (b) **Breach of Agreement:** The need to consult with your client to learn more about the confidentially agreement Doe may have signed.
- (c) **Explore the Extent of Information Leaked:** The need to explore, with your client, any information Doe may have discovered, through his contacts with company.
- (d) **Due Diligence:** The need for disclosure as part of "due diligence" in investigating whether Doe breached confidentiality agreements with the company.
- (e) **Timing:** Point to the timing of certain of Does' messages on the ISP board as circumstantial evidence that Doe had obtained information about confidential business plans through improper means-presumably through his/her previous work or through his/her internal contact at the company.
- (f) **Confidential Figures:** Look to see if "Doe" had disclosed confidential revenue figures on one posting that had only been

provide to Doe's internal contact, on the day before the Internet disclosure.

- (g) **Ownership of Stock:** Argue, if applicable, that Doe's ownership of shares of company stock gave him a motive to manipulate the company's stock price by disclosing trade secrets.

3. Employee Doe's Strategy

In response, if you represent Doe:

- (a) Dispute the confidential nature of the information discussed in messages,
- (b) Argue his/her prediction about corporate revenues was based on public information and was wrong in any event, since Company ultimately announced much different figures (if applicable),
- (c) Argue that speculation about a potential business relationship was a common topic among investors, and
- (d) Challenge company's showing that it had suffered any injury as a result of the alleged disclosures.

III. Employer Claims and Causes of Action

Julie A. Totten

Orrick, Herrington & Sutcliffe LLP
400 Capitol Mall, Suite 3000
Sacramento, CA 95814
tel 916.329.4908
fax 916.329.4900
jatotten@orrick.com

(With special thanks to Alexander Sperry for his valuable assistance.)

Disgruntled current and former employees are turning to electronic communications to attack employers, and frequently their employees, at an alarming rate. Unwilling to simply sit back and take it, however, employers are becoming increasingly more aggressive in responding to cybersmear campaigns with legal action. Moreover, individual employees who have unwittingly been made the targets of cybersmear frequently turn to the courts for protection and redress.

There are numerous theories of liability that may be applicable in a cybersmear suit, depending upon the facts presented. Theories are based both in state and federal statutory law and in common-law principles of tort and contract, and most will support claims for both damages and injunctive relief. Examples of legal theories that have been asserted by plaintiffs in these suits include: defamation, unfair competition, misappropriation of trade secrets, harassment, invasion of privacy, breach of loyalty, breach of contract, appropriation of name, trespass to chattels, trademark and copyright infringement, and intentional infliction of emotional distress. These theories are discussed in more detail below.

A. Defamation

Defamation is frequently asserted to combat Internet cybersmearing. Generally speaking, defamation refers to the act of damaging a person's reputation through the making of false statements, either in writing (libel) or orally (slander). *See Shively v. Bozanich*, 31 Cal. 4th 1230, 1242 (2003) (citing to California's defamation law at Cal. Civ. Code § 44 *et seq.*). Because defamation is a state law tort, its specific definition varies by jurisdiction. While normally asserted by an individual, a company can likewise raise a claim for defamation where it can show that its reputation has been harmed as the result of published misrepresentations.

In the case of *Varian Medical Sys. Inc. v. Delfino*, Varian Medical Systems, Inc., Varian Semiconductor Equipment Associates, Inc. and two of the companies' executives were awarded \$775,000 in compensatory and punitive damages in December 2001 by a jury in Santa Clara, California. The judgment was obtained against two former employees, Michelangelo Delfino and Mary Day, both scientists,

who allegedly posted over 15,000 messages on various message boards using a myriad of different pseudonyms (including some that impersonated company officials). These messages were often repeated on the defendants' web site. The messages asserted, among other things, that (1) Varian and a company executive videotaped employees and children inside a Varian bathroom; (2) Varian fosters a workplace environment characterized by discrimination and harassment; (3) one company executive "sabotaged" a Varian laboratory; (4) another company executive is homophobic and (5) that the same executive would not have hired a woman employee if he had known she was pregnant.

By their acts, the jury found the defendants had committed libel, invasion of privacy (appropriation of name), breach of contract and conspiracy. In addition to the damage award, the judge also issued a permanent injunction barring Delfino and Day from posting additional defamatory messages. Notwithstanding the order, Delfino and Day continued to post defamatory remarks on the Internet and even went so far as to publish a book ("Be Careful Who You SLAPP") about the lawsuit. They also appealed the injunction on the ground that it constituted an unlawful prior restraint. The Court of Appeal agreed that part of the injunction was overly broad since it attempted to prohibit publications that have yet to be composed or deemed defamatory. *See Varian Medical Sys. Inc. v. Delfino*, 113 Cal. App. 4th 273, 305 (2003), *rev. granted*, March 3, 2004. The court did, however, hold that part of Delfino's and Day's remarks were defamatory and upheld the judgment for damages.

HealthSouth Corporation also relied on a defamation theory when it filed suit against John Doe who posted on the Yahoo! Finance message board as I_AM_DIRK_DIGGLER, a reference to the well-endowed porn star in the movie *Boogie Nights*. His postings included statements that the CEO of HealthSouth, Richard Scrushy, was "bilking ...[M]edicare reimbursement" and that the poster was having an affair with Scrushy's wife. In that regard, I_AM_DIRK_DIGGLER wrote that "I am Dirk Diggler and I have what [Richard] Scrushy wants. Too bad I keep giving it to his new wife...[and] [a]s for those of you who disapprove of my crowing about sexual liaisons [sic] with Dick's wife, lighten up, I'm practicing safe sex." *See* Barnett Lidsky, *Silencing John Doe: Defamation & Discourse In Cyberspace*, 49 Duke L.J. at 866-67. HealthSouth sued for libel and commercial disparagement and Richard and Leslie Scrushy filed suit for libel and intentional infliction of emotional distress. *Id.* at 867. As a result of the litigation, HealthSouth learned that I_AM_DIRK_DIGGLER was Peter Krum, a disgruntled former employee. *Id.* at 866.

B. Invasion of Privacy/Appropriation of Name

In addition to defamation, the defendants in *Varian Medical Sys. Inc. v. Delfino*, were also found liable for invasion of privacy (appropriation of name). This tort consists of the following elements: (1) the defendant's use of the plaintiff's name or identity; (2) appropriation of plaintiff's name or likeness for the defendant's

own advantage, commercially or otherwise; (3) unauthorized use or lack of plaintiff's consent; and (4) resulting injury to plaintiff. *See Fairfield v. American Photocopy Equip. Co.*, 138 Cal. App. 2d 82, 86 (1955). In *Varian*, the evidence showed that in posting emails critical of their former employer, many of the defendants' postings were made under the names of their former supervisors without the consent of those individuals, and resulting in their suffering of emotional distress.

In addition, depending on the facts, other privacy torts may also prove useful tools for plaintiffs seeking redress against Internet posters. *See Shulman v. Group W. Productions, Inc.*, 18 Cal. 4th 200, 214 (1998) (involving privacy tort of *public disclosure of private facts*); *Werner v. Times-Mirror Co.*, 193 Cal. App. 2d 111, 119-121 (publicity placing a person in a *false light*); *Dietemann v. Time, Inc.*, 449 F.2d 245, 249 (9th Cir. 1971) (intrusion into a person's *solitude, seclusion or private affairs*).

C. Intentional Infliction of Emotional Distress

As discussed above, oftentimes the disgruntled Internet poster will not limit him or herself to maligning a former employer generally, but will take aim at particular individuals. In these situations, where the content of cybersmear is particularly hurtful or outrageous, and can be shown to have been intended to cause severe emotional distress, a cause of action for intentional infliction of emotional distress may lie. *See Christensen v. Superior Court*, 54 Cal. 3d 868, 903 (1991) (listing the following elements for the tort of intentional infliction of emotional distress under California law: (1) extreme and outrageous conduct by the defendant with the intention of causing, or reckless disregard of the probability of causing, emotional distress; (2) the plaintiff's suffering severe or extreme emotional distress; and (3) actual and proximate causation of the emotional distress by defendant's outrageous conduct).

D. Trespass to Chattels

The tort of trespass to chattels, in essence, prohibits others from substantially interfering with one's personal property, or chattel. To qualify as a trespass, there must be an intentional physical contact with the property of another, which results in substantial interference with, or damage to, that property. *See Thrifty-Tel v. Bezenek*, 46 Cal. App. 4th 1559, 1566-67 (1996). While this cause of action may be useful to companies in combating cybersmear that substantially interferes with or damages a company's electronic communication systems, at least one court has rejected a company's attempt to hold a disgruntled former employee liable under a trespass theory where that former employee sent thousands of disparaging emails to current employees via the company's computer system, but where the company could not show its system had been damaged by such acts. *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (2003).

The *Intel Corp.* case involved a former Intel employee, Kourash Hamidi, who established a web site under the name Former and Current Employees of Intel (www.faceintel.com) and began sending e-mail messages to Intel employees. On six separate occasions, Hamidi sent e-mail messages to 8,000 to 35,000 employees, and in doing so, took steps to evade Intel's attempts to block the messages. The e-mail messages criticized Intel and the company's employment conditions. Intel filed suit for trespass to chattels and sought an injunction prohibiting Hamidi from sending any additional e-mail messages. *Id.* at 1348-50. On appeal, the court affirmed the lower court's grant of an injunction against Hamidi on the grounds that a trespass to chattels had occurred when the e-mails were sent through Intel's computer system and Intel sustained damage when company employees spent time reading and blocking Hamidi's e-mail messages.

The California Supreme Court disagreed. First, it found that Intel failed to show actual and substantial injury to its computer system, more than a momentary or theoretical deprivation of its use. *Id.* at 1357. Second, Intel failed to articulate an injury to its personal property, or to its legal interest in the property, which is required to establish a trespass to chattels cause of action. *Id.* at 1360. Intel's contention that Hamidi hampered its own interest in employee production was not sufficient. Although the Court ultimately refused to recognize Intel's trespass claim, it suggested that Intel could plead under similar facts causes of action for defamation, publication of private facts, or other speech-based torts. *Id.* at 1347-48.

E. Unfair Competition and Misappropriation of Trade Secrets

The term "unfair competition" describes a variety of unlawful conduct that statutes and courts have labeled as illegal business activities, and generally refers to acts that are done dishonestly or unfairly in an effort to harm a competitor. Activities that fall under this label include trade secret misappropriation, unlawful solicitation of a competitor's employees, making false representations in business and false advertising. One of the key risks of cybersmear is that unhappy current or former employees will disclose a company's valuable trade secret information, which is generally not known to competitors. In an effort to prevent further dissemination of confidential information and to collect damages for any consequential loss, companies may file claims for trade secret misappropriation against nefarious Internet posters.

For example, MCSi, Inc., a company working in the audiovisual industry, filed suit in California state court against a competitor, the Whitlock Group, and their employee Robert B. Woods. *See MCSi, Inc. v. Woods*, 290 F. Supp. 2d 1030, 1033-34 (N.D. Cal. 2003). The suit alleged that Woods, who had previously been employed by MCSi's predecessor, had posted negative statements about MCSi and its predecessor in chat room web postings from his desk at Whitlock. MCSi further alleged that not only was Whitlock aware of Woods' conduct, but that it encouraged this behavior in an effort to lure away MCSi's existing and potential customers,

suppliers and investors. Such acts, MCSi contended, constituted both common-law and statutory unfair competition. In response, and after removing the case to federal court, Woods moved to strike the allegations on the basis that MCSi's actions were designed to chill his constitutional free speech rights, pursuant to California's "anti-SLAPP statute." See Cal. Civ. Proc. Code Section 425.16. The court disagreed, concluding that Woods' postings constituted speech by a competitor about a competitor, which were not a matter of public interest deserving of statutory protection.

In February 1999, Raytheon filed suit against 21 John Doe defendants who allegedly posted confidential company matters on an Internet message board, such as information regarding potential mergers and acquisitions, impending divestitures and possible government defense contracts. The postings also included potentially embarrassing information regarding product testing failures. The company asserted, among other claims, a cause of action for misappropriation of its trade secrets, which it alleged caused injury to its business reputation. During the course of discovery, Raytheon learned that nearly all of the Internet posters were employees. Following this discovery, four of the workers quit and the others entered a "corporate counseling" program. Thereafter, Raytheon dismissed the lawsuit. *Raytheon Drops Suit Over Internet Chat*, <http://www.nytimes.com/library/tech/99/05/biztech/articles/22raytheon.html>.

In April 2002, biotechnology company ViroLogic filed a complaint against a Doe defendant alleging he had misappropriated the company's trade secrets by anonymously publishing the company's confidential and proprietary trade secret information on an Internet message board. See *ViroLogic, Inc. v. Doe*, 2004 Cal. App. Unpub. LEXIS 8070 (2004) (unpublished decision). Almost immediately, ViroLogic sought the court's assistance to permit discovery into Doe's identity. At the same time, the Doe defendant filed a special motion to strike the suit, pursuant to California's anti-SLAPP statute. The trial court granted Doe's motion to strike, concluding that ViroLogic's claims arose from Doe's exercise of First Amendment rights in connection with public issues and that ViroLogic had failed to show a probability of prevailing on its claims. In conjunction with this ruling, the court denied ViroLogic's motion to discover Doe's identity. In September 2004, on appeal to the First District Court of Appeal in San Francisco, a three-judge panel reversed the trial court's decision, concluding that the company's right to oppose Doe's anti-SLAPP motion and its claims that Doe may have stolen valuable trade secrets, outweighed the asserted privacy interests of the company's ex-employee who wished to remain anonymous. The court found that had ViroLogic been permitted to fully discover and disclose Doe's identity and investigate fully his relationship to the company, it may have been able to successfully defend Doe's motion.

F. Trademark and Copyright Infringement

Trademark and copyright infringement actions may also provide avenues for redress against cybersmear. In attacking the character or actions of a company, an Internet poster may unlawfully post company-produced material, such as its annual report or confidential memoranda, which may be protected by federal copyright law. *See* 17 U.S.C. § 101 *et seq.* (Federal Copyright Act protects original works of creation that become “fixed in tangible mediums of expression”). In this situation, a company may sue the poster to recover monetary damages for any harm caused by the unauthorized reproduction of its material, and may also seek injunctive relief to prevent or restrain the continued infringement of a copyright. 17 U.S.C. §§ 502, 504.

Moreover, because a business’ name and logo are often the target of Internet cybersmear, federal trademark law may help companies protect their interests and put a halt to damaging Internet activities, including the recent trend of cybersmearers to create website names that “borrow” a company’s moniker to create unflattering web addresses (*e.g.*, [yourcompanynamesucks.com]). However, in the case of *Taubman Co. v. Webfeats*, 319 F.3d 770 (6th Cir. 2003), the Sixth Circuit held that an individual’s creation of websites with domain names that included another company’s name together with the word “sucks” did not violate federal trade mark law, where the website contained both a prominent disclaimer disavowing any affiliation with the plaintiff’s company and provided a direct link to plaintiff’s official web site. The court found that given these protections, there was little likelihood that visitors to his website would be confused as to his affiliation with the plaintiff company, and also that the defendant’s website constituted speech protected by the First Amendment of the US Constitution.

G. Breach of Contract and Breach of the Duty of Loyalty

When the identity of an Internet poster is known or believed to be that of a current or former employee, this may allow a company to also pursue causes of action stemming from the employment relationship. Such charges may include claiming that the employee breached a specific contract that he or she had with the company (such as a confidentiality agreement) or that the employee’s bad acts breached his or her duty of loyalty owed by all employees to their employer. *See Sequoia Vacuum Systems v. Stransky*, 229 Cal. App. 2d 281, 287 (1964) (“Every agent owes his principal the duty of undivided loyalty. During the course of his agency, he may not undertake or participate in activities adverse to the interests of his principal.”)

In *Immunomedics v. Jean Doe, a/k/a “moonshine_fr”*, 775 A.2d 773, 342 N.J. Super. 160 (2001), an anonymous Internet poster, “moonshine_fr,” described herself as a “worried employee” and revealed that the company was “out of stock for diagnostic products in Europe” and that the company was planning to fire one of its executives. Although Immunomedics conceded the truth of these posts, it alleged

that “moonshine_fr” violated the company’s confidentiality agreement and several provisions of the company handbook by these posts. Immunomedics sued, asserting causes of action for breach of contract, breach of the duty of loyalty and negligently revealing confidential and proprietary information. After Immunomedics served a subpoena on Yahoo! to confirm the identity of the anonymous employee poster, “moonshine_fr” filed a motion to quash, contending that a forced disclosure of identify violated the First Amendment. Utilizing guidelines provided by the court in *Dendrite Int’l, Inc. v. John Doe No. 3*, 775 A.2d 756, 342 (N.J. Super. Ct. App. Div. 2001), the motion to quash was denied based upon Immunomedics’ production of evidence demonstrating that “moonshine_fr” was an employee, that all employees execute confidentiality agreements, and the content of the posts that provided evidence of breach of the agreement. Accordingly, the court found that Immunomedics was entitled to disclosure of the poster’s identity. “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,” wrote the court. *Immunomedics*, 775 A.2d 773 at 777-78.

Before engaging in litigation, however, a company should consider both the pros and cons of filing suit. In favor of litigation, a lawsuit may result in the identification of the author, which in turn, may subdue the Internet poster responsible for the harmful campaign. Additionally, once the online poster is identified, the company may be able to reach an agreement with that individual whereby the lawsuit is dismissed in exchange for an agreement to refrain from posting additional defamatory or disparaging material. Filing suit also sends a clear message to other potential posters that defamatory conduct will not be tolerated.

Not to be overlooked, however, lawsuits may also have the unintended affect of causing the Internet poster to increase the number of negative postings regarding the company, and may negatively affect employee morale. Additionally, in response to litigation, the online poster may file a countersuit alleging any number of theories, such as wrongful termination, discrimination, harassment, securities violations and theories based on applicable state laws regarding Strategic Litigation Against Public Participation (“SLAPP”). In doing so, the online poster may receive assistance from groups such as the Electronic Privacy Information Center (www.epic.org) and the American Civil Liberties Union (www.aclu.org). Also at risk is the very real possibility that the online poster will use the discovery process to attempt to depose numerous company officials, including high-level executives. If defamation is alleged by any individual plaintiffs, the online poster will most likely be permitted to conduct discovery into the truth of his or her allegations, which may constitute sensitive and private information. In the end, a company may decide that the expense and trouble of litigation may outweigh its potential benefit.

IV. Employee Defenses and Related Considerations

Mark D. Risk, Esq.
Filippatos Risk LLP
60 E. 42nd St., 47th Floor
New York, NY 10165
212-682-2400
mdr@filippatosrisk.com

The private sector, at will employee has no First Amendment rights against her employer, and barring some other statutory protection can be terminated based upon the content of her speech.

The peculiar feature of cybersmear employment litigation -- that the case is directed principally at discovering the names of the offending employees -- has strategic consequences for the employee who wishes to communicate about his employer on the internet. Attorneys defending employees in cybersmear actions, be they disclosed or anonymous defendants, should also consider the possibility that additional defenses are available under various statutes.

A. Anticipating a Subpoena upon the ISP

Since discovery does not normally take place until after the defendant is served, Courts have attempted to set forth criteria under which pre-service discovery of the third party internet service provider will be permitted in order to permit the plaintiff to determine the identity of the defendant. Employees could protect themselves in these actions by considering that they ought not to reveal that they are employees of the company, and by being careful not to make libelous statements.

In *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999), a trademark action, the court noted that Americans have the right to act “pseudonymously and anonymously” as long as their actions are within the law. The court set forth four requirements in connection with pre-service requests for discovery from the ISP.

1) to insure jurisdiction and justiceability of the dispute in federal court, the plaintiff should identify the missing party with sufficient specificity that the Court can determine that defendant is a real person or entity who could be sued in a federal court.

2) to protect the right to service of process, the plaintiff should identify all prior steps taken to identify and to serve process upon the defendant. This is to protect the right to service of process.

3) to protect the defendant from the unfairness of ex parte adjudication, the plaintiff must establish that the suit could withstand a motion to dismiss.

4) the plaintiff should submit its discovery request to the Court, and state the reasons for the specific discovery requested, identify a limited number of persons or entities on whom discovery process might be served and for which there is reasonable likelihood of producing the identifying information that would make service of process possible.

Following *Columbia Insurance*, in *Dendrite International Inc. v. John Doe No. 3*, 342 N.J. super 134 (N.J. Super A.D. 2001), a New Jersey appellate court considered a request for discovery served upon Yahoo! to determine the identity of a defendant who was posting critical comments on a Yahoo bulletin board. The *Dendrite* requirements were directed at protecting the First Amendment right of anonymous speakers, but were similar to the *Columbia Insurance* requirements:

1) the plaintiff must first take efforts to notify the anonymous posters that they are the subject of a subpoena for disclosure, and give them time to oppose the application.

2) the plaintiff must set forth the exact statements purportedly made that constitute actionable speech, and produce sufficient evidence supporting each element of its cause of action. This includes the element of damages.

3) if the court determines that the plaintiff has presented a prima facie cause of action, it must then balance the First Amendment right of anonymous speech against the strength of the prima facie case and the necessity for disclosure of the identity of the anonymous defendant in order for the plaintiff to proceed.

The court found that the plaintiff could not show that it had suffered any damages by virtue of the posted statements by John Doe #3. *Dendrite's requirement* that the employer must make a preliminary showing of its damages will make it much more difficult for the employer to prevail on a third party subpoena application where the underlying claim is defamation. Employees who post comments on the Internet would help themselves by showing prudence in what they post, trying not to make defamatory statements about the employer that would cause the employer measurable economic damage.

Interestingly, however, in *Immunomedics, Inc. v. Doe*, 342 N.J. Super. 160 (N.J. Super. 2001) the same New Jersey court distinguished *Dendrite* and denied the motion by an anonymous internet user to quash the subpoena served upon the ISP to reveal her identity. The distinguishing feature was that the anonymous user had identified herself as an employee of plaintiff, and the causes of action were for breach of the confidentiality provisions of the employee handbook as well as the common law duty of loyalty. These claims were ruled sufficient to outweigh the employee's First Amendment protections. *Immunomedics* suggests that an

employer is much more likely to succeed in subpoenaing the ISP where it can assert contract or fiduciary claims arising directly from the employment relationship. Ironically, it also suggests that Internet posters should consider not revealing themselves as current employees of the company they are criticizing.

Employees have generally been permitted to move anonymously to quash the subpoena served upon the ISP. *See Doe v. 2TheMart.Com Inc.*, 140 F. Supp. 2d 1088, 1091 (W.D.Wash. 2001), *America Online, Inc.*, 542 S.E. 2d 377 (Va. Sup. Ct. 2001) (corporate plaintiff may proceed anonymously on defamation claim).

B. Anti-SLAPP statutes

Many states have enacted statutes allowing for an early motion by a defendant to dismiss lawsuits directed at the exercise of First Amendment rights to speak on matters of public interest. The original statute was California's anti-SLAPP statute (directed at "Strategic Lawsuits Against Public Participation"). These statutes require special showings in a manner similar to the *Dendrite* First Amendment requirements, and may be useful to the employee even after the employer has obtained her identity.

In *Baxter v. Scott*, 847 So. 2d 225 (La. Ct. App. 2003), the administrator of a public university brought a defamation action against the author of a website who alleged mismanagement and abuse of office by members of the administration. Originally a "John Doe" case, plaintiff amended the complaint to allege claims against John Scott, a former professor at the university.

The SLAPP statute works like this. Defendant can make an immediate motion to dismiss the claim(s). He must make a prima facie showing that the claim arises from an act in furtherance of his rights of petition or free speech in connection with a public issue as defined by the statute. If successful, the burden shifts to the plaintiff to demonstrate a probability that he will prevail on the merits. Plaintiff must state and substantiate a legally sufficient claim, by making a prima facie showing of facts sufficient to sustain a judgment in its favor.

In *Baxter*, plaintiff claimed that Scott's statements fell outside the protections of the statute. The court noted that the website was open to the public, and that the public has an interest in a public university that both receives public funding and contributes to the economy of the area in which it is located . . . and whether it is having financial difficulties that are possibly being misrepresented to the public." *Id.*, at 233.

To substantiate the defamation claim, plaintiff must address all of the elements of that claim: 1) a false or defamatory statement, 2) unprivileged publication to a third party, 3) fault of the publisher, and 4) resulting injury. The court further noted that speech on matters of public concern enjoys enhanced constitutional protection, *citing Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc*

472 U.S. 749 (1985). Hyperbole is a specifically protected form of speech. *Greenbelt Cooperating Publishing Ass'n v. Bressler*, 398 U.S. 6 (1970).

The appellate court reversed the trial court and dismissed the case. In defamation actions the anti-SLAPP statutes impose hurdles on the plaintiff requirements similar to those imposed by *Columbia Insurance* and *Dendrite*.

C. NLRA Concerted Activity

An employee whose anonymous internet speech focuses on wages, hours, working conditions and other matters of common employee concern is probably engaging in activity protected by the National Labor Relations Act.

Section 7 of the National Labor Relations Act makes it unlawful to interfere with employee concerted activity in pursuit of mutual aid or protection. Although the touchstone of the protection is that the activity must be “looking toward group action,” the object of inducing group action “not need to be express.” *Id.* The right is enforced via the filing of unfair labor practice charges with the NLRB, but it is applied to protect employees in non-union as well as union settings.

In *Timekeeping Systems, Inc.*, 323 NLRB No 30 (1997), after inviting employees to reply and comment on proposed changes in the vacation policy, it terminated an employee who replied by writing to all employees by email that a change in the company’s vacation policy was not advantageous for employees. Management claimed to object to a tone of disrespect in the emails rather than their substance.

The NLRB ruled that the email messages were concerted activity, since they were clearly directed at inducing the other employees to assist in preserving the former vacation policy. The Board affirmed the Administrative Law Judge’s decision including the finding from the evidence that the employer’s decision to terminate the employee was related to the concerted nature of his activities.

Some concerted conduct involving speech can be expressed in a manner so intolerable that it loses its Section 7 protection, if found “to be so violent or of such serious character as to render the employee unfit for further service,” *Dreis & Krump Mfg. Co. v. NLRB*, 544 F.2d 320 (7th Cir.1976). The Board and reviewing courts have applied this exception very narrowly, only where the concerted behavior is “truly insubordinate or disruptive of the work process.” Expressions of anger or personal attacks have generally been deemed protected.

In the extraordinary case of *Konop v. Hawaiian Airlines, Inc.*, 302 F. 3d 868 (9th Cir. 2002), an airline pilot brought a pro se action against his employer after a vice president had gained unauthorized access to a secure website he maintained and disclosed its contents. He contended that the employer had violated the anti-retaliation provisions of the Railway Labor Act by terminating him after seeing the

website. He also contended that the employer's actions had violated the federal Stored Communications Act (*see infra*).

Konop created and maintained a website for the posting of bulletins critical of his employer Hawaiian Airlines ("Hawaiian"). Much of the material concerned criticisms of certain concessions that Hawaiian sought from their union, the Airline Pilots Association ("ALPA"), and suggested that the Hawaiian workers consider joining another union.

Access to the website was limited to a list of employees, and required that they choose passwords. To receive a password the user would have to indicate agreement to certain terms of use, including that members of Hawaiian's management were prohibited from viewing the website. A member of management accessed the site simply by entering the name of one of the employees who had not yet accessed the site, and then choosing a password, thereby indicating acceptance of the terms and conditions of use.

Within hours, the president of Hawaiian had contacted the chairman of ALPA, who phoned Konop. Hawaiian was upset by comments and accusations on the website and had threatened to sue for defamation. Konop claimed not to have known how Hawaiian had gotten this information, and took the site off line for only a day, then put it back on line. Over the next four months, two Hawaiian executives logged in to the website about 34 times, using the names of two pilots, with their consent.

Konop sued Hawaiian contending that its unauthorized access to his secure website was unlawful, and that Hawaiian's placing him on "medical suspension" was in retaliation for his opposition to the requested contract concessions. The district court granted summary judgment to Hawaiian on all claims except the retaliatory suspension claim, which it dismissed after a short bench trial.

The Ninth Circuit reversed the decision on the Railway Labor Act ("RLA") claim, finding that triable issues existed as to whether Hawaiian's conduct violated the RLA, and reinstated Konop's counterclaim under the Stored Communications Act (*see infra*).

The RLA prohibits employers from "interfering in any way with the organization of its employees," See 45 U.S.C. § 152. Konop alleges that Hawaiian violated the law by each of i) the unauthorized access to his website, ii) by disclosing its contents to the Airline Pilots Union, thereby wrongfully assisting or favoring it, iii) and by threatening to file a defamation suit against Konop based on the statements on the website.

Hawaiian argued that Konop forfeited his protection under the RLA because his postings contained "malicious, defamatory and insulting material known to be false." 302 F. 3d at 882, *citing Linn v. United Plant Guard Workers Local 114*, 383

U.S. 53,61 (1966) (NLRA protections forfeited by employee “circulating defamatory material known to be false.”) Konop had compared Hawaiian’s management to the Nazis and the Soviets, and described its president as “one incompetent at the top” with “little skill and little ability with people.” It also said that Hawaiian’s president was suspected of fraud.

The Ninth Circuit found, however, that most of the statements objected to by Hawaiian were non-defamatory and specifically protected as either hyperbole or opinion. “Federal law gives a union license to use intemperate, abusive, or insulting language without fear of restraint or penalty”, *quoting San Antonio Comm. Hospital v. S. Cal. Dist. Council of Carpenters*, 125 F 3d 1230, 1235, *quoting National Ass’n of Letter Carriers v. Austin*, 418 U.S. 264, 282-83 (1974). The most problematic of Konop’s statements was the claim that the airline president had been suspected of fraud, but the Ninth Circuit found it non-defamatory because Hawaiian had presented no evidence that Konop knew that the statement was false. Federal labor law protects false and defamatory statements unless they are made with knowledge of their falsity or reckless disregard for the truth. *Konop* at 883, *citing Letter Carriers*, 418 U.S. at 281. The court also found triable issues of fact, based on the testimony of the ALPA chairman, on the claims that Hawaiian unlawfully assisted ALPA by disclosing the contents of Konop’s website, and by threatening the defamation suit. The court affirmed the dismissal of the retaliation claim, on the grounds that Konop had not produced sufficient evidence that he was placed on medical leave in retaliation for his website.

Employees who wish to discuss their employer on the Internet would do well to limit their statements to matters arguably protected by the labor laws. They could use their NLRA statutory protections as additional arguments in their motions to quash subpoenas served upon the ISP, since these protections augment and underscore their First Amendment rights.

D. Whistleblower Statutes and the Sarbanes Oxley Act

Section 806 of the Sarbanes Oxley Act, 18 U.S.C. § 1514A, protects employees of publicly traded companies from retaliation for investigating or reporting a wide range of fraudulent activity, including securities fraud, bank fraud, mail or wire fraud, violation of any SEC rule or regulation, or of any federal law provisions related to fraud on shareholders. The reporting could be to a federal agency, a member of Congress, or to someone within the company “with supervisory authority” over the reporting employee. The statute provides for the filing of an administrative complaint with the Department of Labor, and then maintenance of a private lawsuit 180 days later if the DOL has not proceeded through a hearing and appeal on the matter.

It is unlikely that the posting of information on an internet website could be deemed among the employee activity protected by the Act. Employees must

understand that the mere knowing or talking about unlawful practices is not sufficient to invoke the protections of either the Sarbanes Oxley Act or, for that matter, most other whistleblower statutes. On the other hand, an employer seeking to act against allegations on the Internet concerning unlawful practices should be mindful that if the same employee has also made a proper complaint wither within the company or to an appropriate government agency, then taking action against the internet activity may expose it to a claim of whistleblower retaliation, particularly where the employer is aware of the employee's complaint prior to taking the action.

Numerous other federal statutes have whistleblower protection provisions, which could be invoked based upon the communication at issue. These include the False Claims Act, 31 U.S.C. § 3729 et seq.; Energy Reorganization Act, 42 U.S.C. § 5851(a)(1)(D); Clean Air Act, 42 U.S.C. § 7622(a)(1); Safe Drinking Water Act, 42 U.S.C. § 300j-9(i)(1)(A); Solid Waste Disposal Act, 42 U.S.C. § 6971; Toxic Substance Control Act, 15 U.S.C. § 2622. In addition, state law whistleblower statutes may also apply to employee web site postings.

Of course, most whistleblower statutes require formal disclosure, or intended formal disclosure, in proceedings related to the alleged unlawful activity, and an employee would be foolish to conclude that whistleblower statutes absolutely permit him to post allegations against her employer on the internet. On the other hand, employers should be mindful of applicable whistleblower statutes in deciding how to respond to employee material on a website.

E. Stored Communications Act Counterclaim

Unauthorized access by an employer to a secure website maintained by an employee may be unlawful under the federal Stored Communications Act.

In *Konop* (*see above*) the airline pilot plaintiff also alleged that Hawaiian violated the federal Wiretap Act, 18 U.S.C. § 2510-2522 and/or the Stored Communications Act, 18 U.S.C. § 2701-2711 when its executive accessed Konop's secure website. The Ninth Circuit struggled with the interplay between these statutes, concluding, over a lengthy dissent by Judge Reinhardt, that the Wiretap Act does not impose penalties with respect to the interception of stored electronic communications. *See Konop*, 302 F.3d 876-879, and Judge Reinhardt's dissent at pp. 886-892.

The Stored Communications Act prohibits intentional "access without authorization [to] a facility through an electronic communication service is provided. . . and thereby obtain. . . access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a)(1).

There was no dispute that Konop's website was covered by the statute, or that the executives' access was unauthorized. The issue considered by the Ninth

Circuit was whether Hawaiian was covered by a provision in the statute that exempts “conduct authorized . . . by a user of that service with respect to a communication of or intended for that user.” 18 U.S.C. § 2701(c)(2). Simply put, did the fact that two covered employees gave permission to the Hawaiian executives to use their names and access the site take the executives’ actions outside the coverage of the statute?

The Ninth Circuit noted that various parts of the Wiretap Act and the Stored Communications Act as well as their legislative history expressed the principle that an intended recipient of an electronic communication could authorize third parties to access that communication. However, the Court refused to depart from the plain language of the Stored Communications Act, which defines a “user” as someone who both uses the service and is authorized to do so. 18 U.S.C. § 2701 (c)(2). The Ninth Circuit found that there was no evidence that the two pilots who allowed the employer to use their names to access Konop’s website had ever themselves used the site, and that therefore they were not “users” under the statute with the power to authorize others. *Id.*, 302 F. 3d at 879-81. The court reinstated Konop’s claim under the Stored Communications Act.

Konop suggests that employees using a secure website to discuss with co-workers matters related to their employment have added protections against employer action.