



## Cyber-Defamation: It's Not Just Business as Usual

By Zachary G. Newman and Anthony Ellis

From starting up Facebook pages (Coca Cola has 20 million “fans”) to establishing “Twitter” accounts (Google has 2.6 million “followers”), businesses around the world are embracing the Internet and the many marketing and business opportunities it presents. Yet, businesses are also learning that the same reasons that caused them to flock to the Internet—the ability to reach millions of people in a quick and efficient manner—can also be an Achilles’ heel. To paraphrase an old idiom, the Internet is just a publishing house, and all the men and women are potential publishers. Never before has it been so easy to reach so many with such limited effort, and the simple fact is that many of those publishers are acting with both animus and anonymity.

Anticompetitive and tortious behavior abounds. Competitors are posing as fake customers, spreading false and highly damaging rumors about companies, their personnel, and their products. Consumers are utilizing company Facebook accounts and Twitter postings to levy complaints, both legitimate and illegitimate (a particular problem in our age, where purchasing decisions are increasingly based upon user reviews). In addition to these external hazards, companies are facing internal threats from their own employees. Company employees are starting so-called gripe sites to complain and critique company personnel and policies. *See, e.g., Pietrylo v. Hillstone Restaurant Group*, No. 2:06-cv-5754, 2009 U.S. Dist. LEXIS 88702 (D. N.J. Sept. 25, 2009) (former employees of the Houston’s restaurant sued their former employer when managers fired them after discovering that the employees created a password-protected gripe site to complain about the company. The employees were awarded punitive and compensatory damages based on the managers’ access of the password-protected site, despite the fact that the log-in information used by the managers to access the site was freely given by a fellow employee). The written word on the Internet seems to carry instant credibility, and smart companies are becoming hyper-vigilant in protecting their reputations and defending against illegitimate posts.

In this context, we as lawyers are being consulted about cyber-claims, and particularly cyber-defamation claims. You may be approached by a company that simply wants to know what legal recourse is available to stem a smear campaign. In other cases, clients may feel victimized or personally affronted (particularly

in the case of a competitor) and want you to use “all means necessary” to take down the defamer and those that facilitated the defamation. Before treading into the world of cyber-defamation litigation, you should be aware of the complex and unique procedural and statutory rules governing such claims in addition to those already inherent in prosecuting or defending defamation claims. For a plaintiff, these rules may mean that there is no pot of gold at the end of the rainbow; the only pot of gold is the money that your client spent chasing down the alleged defamer without success. For a defendant, there are a number of potential jurisdictional and statutory defenses that could allow your client to escape from such litigation quickly and without significant expense, but to the extent that they are ultimately found liable, there may be significant damage awards for what may appear to your client to be a fairly insignificant statement that is found to be defamatory and actionable.

### Does the Claim Satisfy the Basic Elements of Defamation?

At the outset of any potential claim, it is important to understand that the foundation for these cyber-based claims is defamation law. The exact contours of a defamation claim, commonly referred to as libel for published defamation, and the specific causes of action available to a plaintiff will generally depend on the specific law that applies. In general, however, the basic elements of a defamation claim have not changed in the Internet context. A plaintiff generally needs to establish that a false statement of fact published to someone other than the plaintiff is derogatory or otherwise harms the reputation of the plaintiff; the publisher bore fault for the statement, either through negligently publishing it or acting maliciously; and the plaintiff was damaged as a result of the statements. *See, e.g., Harris v. Bornhorst*, 513 F.3d 503, 522 (6th Cir. 2008); *Bustos v. United States*, 257 F.R.D. 617, 621 (D. Colo. 2009); *Singer v. Beach Trading Co.*, 876 A.2d 885, 894 (N.J. Super. Ct. App. Div. 2005). If the statements were made about a public figure, then the plaintiff would also need to establish actual malice. *See New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).

Many states recognize categories of statements that are considered so inherently derogatory that they are per se defamatory, so the plaintiff does not need to establish any special damages. Disparaging statements about a person’s criminal

record, sexual history, and trade or occupation are generally considered defamation per se. *See, e.g., Snyder v. Ag Trucking, Inc.*, 57 F.3d 484, 489 (6th Cir. 1995). Outside of such statements, however, it is critical for the attorney to make at least an initial assessment of whether the statement at issue is a statement of opinion that would likely be considered constitutionally protected speech or an actionable false statement of fact. For many derogatory statements, there may be some court precedent on the type of claim at issue that may provide the lawyer with guidance on how a court would resolve the issue. Without any precedent, however, this is often no easy task. What constitutes an opinion versus a factual statement has been the subject of numerous articles and cases over the years, and court dockets are rife with expensive and time-consuming lawsuits ending with a defense verdict or dismissal.

Moreover, truth is an absolute defense to a defamation claim, and the burden of whether the plaintiff or the defendant is obligated to prove the truth or falsity of the statement depends upon the type of claim brought. As a plaintiff, it is important to discuss and consider whether your client really wants to get into a public trial about whether the claimed defamatory statements are true. In addition, statements made in the context of a lawsuit or litigation, such as affidavits or declarations, are generally immune and privileged from defamation claims (although similar comments made to friends, acquaintances, posted online, or emailed are not). Other defenses are also available in certain jurisdictions.

Even if the potential statement was defamatory, this is merely the tip of the iceberg in determining whether, who, and where to sue, and if such a suit is commenced against your client, how you could get him or her out of the litigation.

### Personal Jurisdiction in the Cyber-Defamation Context

Jurisdiction in the cyber-defamation context is not a settled issue, and courts are attempting to come to grips with the various unique issues pertaining to Internet jurisdiction generally, such as “where” something was said and “where” someone was harmed. Because of the global nature of the Internet, this is an issue that is being addressed not only by state and federal courts in the United States, but also in jurisdictions around the world. For example, what is the proper forum for dealing with a case between a Canadian citizen who purportedly spread defamatory statements about an Indiana business to a friend in India through a website owned by a Chinese company using a server based in Vietnam that the Indiana business owners learned about while on a computer in South Africa? The analysis of the proper or available jurisdictions can be dizzying and requires careful research to avoid a costly jurisdictional mistake or fight.

In the United States, jurisdiction prerequisites differ by state. Some states have adopted laws providing for jurisdiction over a cyber-defamer to the extent that the party targets people living in that state. *See Clemens v. McNamee*, 615 F.3d 374, 379 (5th

Cir. 2010) (finding that to exercise jurisdiction in Texas against a nonresident defendant, the forum must be the “focal point” of the story either by making the statements in Texas or directing the statements to Texas residents’ conduct in Texas, thus rejecting Clemens’s attempts to obtain jurisdiction over McNamee in Texas) (citing *Calder v. Jones*, 465 U.S. 783 (1984) (holding that a California court could exercise jurisdiction over a gossip columnist because the publisher expressly aimed its defamatory comments at a California resident)). For example, if a cyber-defamer commented that Bob Smith, who lived in Fort Worth, Texas, was a criminal, courts utilizing the “targeting approach” would likely find a sufficient nexus to exercise personal jurisdiction in Texas. If, however, the cyber-defamer merely criticized Bob Smith, without referencing his residence or otherwise connecting his residence to the post, then Bob Smith may have a more difficult time hauling the cyber-defamer into court in Texas. Other states have adopted entirely different approaches, permitting, for example, a plaintiff to bring suit as long as the defamed party’s reputation was damaged in that particular state. *Kauffman Racing Equipment v. Roberts*, 930 N.E.2d 784 (Ohio 2010). In those states, a cyber-defamer who lives in Maine and has never left Maine could be hauled into court in Ohio if he or she posted information that ultimately caused the plaintiff some reputational harm in Ohio (for example, posting negative comments about an Ohio business from the comfort of the defendant’s Maine living room). *Id.*

In addition to the question of whether a party could be haled into a particular forum as a defendant, there is the independent and equally important consideration of how that particular forum addresses legal issues surrounding the defamation claim, such as the statute of limitations. For example, if the allegedly defamatory statement was initially posted on a public but little-known website three years ago but only made its way onto the *Wall Street Journal’s* website (where your client noticed it) one month ago, how will the potential forum treat that claim? In the context of cyber-defamation, a plaintiff may simply not know when the “first” publication of the defamatory statement was made.

Yet, to date, courts have uniformly adhered to a “single publication” rule, meaning that with the first publication of the statement, the statute of limitations begins to accrue. *Wolk v. Olson*, No. 2:09-cv-4001, 2010 U.S. Dist. LEXIS 77694 (E.D. Pa. Aug. 2, 2010 (“The Court is not aware of any case in which the discovery rule has been applied to postpone the accrual of a cause of action based upon the publication of a defamatory statement contained in a book or newspaper or other mass medium. I reach the same conclusion as my colleagues in the Eastern District of Pennsylvania and other jurisdictions: as a matter of law, the discovery rule does not apply to toll the statute of limitations for mass-media defamation.”) (citing cases). Thus, the statute of limitations for defamation may become a critical issue in choosing where to litigate such a claim. For

a full list of state statutes of limitations for Internet libel and the corresponding citations, see Rexxfield, LLC, Internet Libel Statute of Limitations, [www.rexxfield.com/internet\\_libel\\_statute\\_of\\_limitations.php](http://www.rexxfield.com/internet_libel_statute_of_limitations.php).

For a potential plaintiff, there is also the question of whether to sue in state court, federal court, or courts of lower jurisdiction (such as small-claims court, county courts, or town courts). Local courts of limited jurisdiction may offer a fast and efficient way for a client to redress his or her grievances. With respect to equitable relief, however, it is important to remember that some of these courts are not able to award equitable relief, such as ordering the removal of the defaming language from the Internet (although some could potentially condition a specific damages award on some particular action such as removing the defaming statement from the Internet). Simple and streamlined cases in courts that have the capacity to litigate expeditiously could be the perfect formula for redress in these circumstances.

Identifying the speaker is not as easy as it may sound. Many posts are made anonymously or through an untraceable screen name.

Jurisdictional issues are even more complicated when you factor in potential international forums. Internet defamation can easily target and harm a business or corporation throughout the world, and depending upon the source and the size of the defamer, these cases can easily find themselves in foreign courts. Should you consider and discuss with your client the costs, benefits, and potential pitfalls of commencing suit in the United Kingdom, Australia, or even Canada, assuming that they were able to satisfy the jurisdictional prerequisites? If a claim is barred in the United States, could it be pursued abroad? Globally, each country, and perhaps each province, state, or territory within that country, may have its own jurisdictional requirements, and in the context of a global defamation claim, U.S. lawyers practicing in this arena may quickly become familiar with these standards as well. Given that significant libel and defamation awards have been handed down by foreign courts, depending on the specific standards and statute of limitations issues, your client's best or most appropriate opportunity at redress may be in a foreign jurisdiction. See, e.g., *Totalise plc v. Motley Fool Ltd.*, [2001] EWCA Civ 1897 (appeal taken from Q.B.) (U.K.), available at [www.bailii.org/ew/cases/EWCA/Civ/2001/1897.html](http://www.bailii.org/ew/cases/EWCA/Civ/2001/1897.html) (demanding disclosure of anonymous bloggers and ordering bloggers to

pay the plaintiff's attorney fees); *Black v. Breeden*, [2010] ONCA 547 (Can.), available at [www.ontariocourts.on.ca/decisions/2010/august/2010ONCA0547.htm](http://www.ontariocourts.on.ca/decisions/2010/august/2010ONCA0547.htm) (rejecting jurisdictional challenge and permitting Conrad Black to proceed in a libel suit against Hollinger International in Ontario based on the theory that the republishing of Hollinger International press releases by papers distributed in Canada caused him harm in that province).

### Cyber-Defamation Defendants

#### *The Speaker*

Although you may think that the defendant in the cyber-defamation context is clearly the speaker (or writer), this is often not the case. In the cyber-world, identifying the speaker is not as easy as it may sound. Many posts are made anonymously or through an untraceable screen name.

To identify anonymous speakers, parties, depending on the applicable procedural rules, can commence suits against John or Jane Doe and begin using subpoena power on the service providers and host sites. See, e.g., *Doe I and Doe II v. Individuals*, 561 F. Supp.2d 249 (D. Conn. 2008). Pre-action discovery could also be available, depending on the jurisdiction. See John P. McCahey and Anting Wang, Hahn & Hessen, LLP, *Pre-Action Discovery in the Digital Age*, 2009 LexisNexis Emerging Issues 4554 (Nov. 2009). But be warned, this is not a simple assignment. Courts have recognized that, as in the traditional speech context, the First Amendment protections afforded to anonymous speech extend to the Internet arena. Because the Supreme Court simply has not addressed the proper standard for balancing the free speech rights of the anonymous speaker against the right of the defamed plaintiff to redress, courts have developed a wide variety of standards for addressing the issue. Some courts, for instance, have created a set of enumerated factors. See *Enterline v. Pocono Medical Center*, No. 3:08-cv-1934, 2008 U.S. Dist. LEXIS 100033 (M.D. Pa. 2008) (applying a four-part test); *Doe I*, 561 F. Supp. 2d at 254–55 (setting forth a six-factor test). Other courts have adopted a fairly strict test, requiring the party to establish that he or she would be able to prevail on a motion for summary judgment for all elements of their defamation claim based upon evidence within its control—i.e., “not dependent on knowing the identity of the poster.” See, e.g., *Ecommerce Innovations, LLC v. Doe*, No. MC-08-93-PHX-DGC, 2008 U.S. Dist. LEXIS 99325 (D. Ariz. Nov. 25, 2008).

Another consideration is that while some courts have ordered the disclosure of otherwise anonymous posters, pursuing the name of the speaker through litigation could be very expensive and time-consuming. *In re Anonymous Online Speakers, Anonymous Online Speakers v. United States District Court for the District of Nevada Reno*, 611 F.3d 653 (9th Cir. 2010) (affirming a district court order requiring an online content manager to disclose the identifies of certain comment posters based on allegations by a business that its competitors were engaging in an anonymous smear campaign to injure its reputation); *In re*

*Subpoena Duces Tecum to Am. Online, Inc.*, 52 Va. Cir. 26 (Va. Cir. Ct. 2000) (ordering the disclosure of identities from the ISP of parties that allegedly disclosed confidential trade secrets and defamed the business), rev'd on other grounds by *America Online, Inc. v. Anonymous Publicly Traded Co.*, 542 S.E.2d 377 (Va. 2001).

As counsel, you should discuss with your client whether, from an economic standpoint, it makes financial sense to initiate a lawsuit. For example, if the defamer is someone who is likely to be judgment-proof, obtaining a monetary judgment against him or her may have little benefit for your client. Given the costs associated with such discovery, you also need to determine whether your investigation should include efforts to identify potential defendants that may have facilitated or republished the defamatory statements. You will likely have to justify your actions to your client, particularly if your efforts fail to uncover the perpetrator, so you should make sure up front that both you and your client are comfortable with and confident in the discovery plan to be followed. From a defense perspective, if you find yourself in receipt of one of these subpoenas, your client may or may not be compelled to divulge information about its customers, as the law differs from jurisdiction to jurisdiction.

Best practices mandate that the lawyer conduct a thorough review of the law pertaining to these types of disclosures, understand recent decisions that can impact strategy, and fully explain to the client the legal risks, benefits, and projected costs.

One potential avenue that could avoid the costs and expenses of litigation is retaining a third-party consultant or investigator to assist in identifying the speakers. Dozens of firms are sprouting up as these suits become more and more common, and many of them boast of significant success in identifying the perpetrators. See, e.g., REXXFIELD, LLC, Digital Forensics, Investigations & Litigation Support, [www.rexxfield.com/libel\\_law\\_suit.php](http://www.rexxfield.com/libel_law_suit.php) (noting that “in most Doe cases (unidentified defendants) we can positively identify the offenders using proprietary investigative techniques as well as carefully crafted subpoenas and orders, and noting an 80–90% success rate”).

#### *The Internet Service Provider*

In addition to the speaker or poster of the information, there could be a claim available against web hosting services and Internet Service Providers (ISPs) for the websites where the comments were posted on the theory that they republished the incriminating statements. Initially, it may seem like an easy decision to sue the ISP—financial recovery may seem more likely from an ISP than from the creator of the post—but there are in fact significant statutory defenses available to such service providers in the context of cyber-defamation claims.

Section 230 of the Federal Communication Decency Act of 1996 (CDA) explicitly provides that “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider” (CDA, 47 U.S.C. § 230(c)(1) (1996)), and

further that “no cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.” § 230(e)(3). Based on this language, courts have regularly dismissed claims against websites that post third-party comments and information that were allegedly defamatory. See, e.g., *Reit v. Yelp!, Inc.*, 907 N.Y.S.2d 411 (N.Y. Sup. Ct. 2010) (dismissing a defamation claim against Yelp! for allegedly defamatory negative comments about the plaintiff’s dental practice). A highly regarded Internet defamation lawyer and author, Aaron Morris, has used the very apt analogy that “naming an Internet Service Provider in an Internet defamation action is akin to naming Microsoft as a defendant because the defamer used Word to type the defamatory statements.” See <http://internetdefamationblog.com>.

Whether the website host is ultimately immune from a defamation suit will likely depend on the level of involvement it has or had with the speech and speakers who post on its site and whether the website arguably was involved in encouraging illegal conduct. In one noteworthy recent case from the Ninth Circuit, *Fair Housing Council of San Fernando Valley v. Roommate.com, LLC*, 521 F.3d 1157 (9th Cir. 2008), the court held that because Roommate.com’s website was structured in such a way that users submitted information that was then posted by Roommate.com, the website crossed over from being merely an interactive computer service (with no liability for the statements) to being an information content provider that could potentially be liable for defamatory posts on its site. Yet, even getting to the position where you can tell the type of information service provider with which you are dealing may itself require significant amounts of time and the retention of an expert who can navigate the technical details and nuances of the posting technology.

#### **Anti-SLAPP Laws**

Another aspect of potential defamation claims is what are commonly referred to as anti-SLAPP laws. Strategic lawsuits against public participation (SLAPP) are designed to silence people from making otherwise protected but unwanted speech, such as legitimate consumer opinions or complaints. California led the United States with anti-SLAPP litigation, offering potential defendants an allegedly quick and efficient means of dismissing such complaints. Cal. Civ. Pro. § 425.16. If the alleged defamation fell within a specific category of protected statements, defendants could file a short motion establishing that the speech was protected and effectively stay all discovery pending resolution of the motion. If the motion is denied, the order is immediately appealable. If the defendant prevailed, then the plaintiff is obligated to pay for the defendant’s attorney fees. Ultimately, faced with what many people considered abuse of anti-SLAPP legislation, California carved out from the procedure suits involving commercial issues and made other changes to the anti-SLAPP legislation, but this provision

remains an important potential consideration for anyone considering filing a defamation suit. Cal. Civ. Pro. § 425.17.

Twenty-six states, including Arizona, Arkansas, Delaware, Florida, Georgia, Hawaii, Illinois, Indiana, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Missouri, Nebraska, Nevada, New Mexico, New York, Oklahoma, Oregon, Pennsylvania, Rhode Island, Tennessee, Utah, Vermont, and Washington, have enacted their own anti-SLAPP legislation, and Colorado and West Virginia have adopted non-statutory protections against SLAPP lawsuits. Similar legislation has been introduced at the federal level. See The Citizen Participation Act, H.R. 4364, 111th Cong. (2009). In any case, in determining where and whether to file suit, counsel should consider the relevant anti-SLAPP legislation and its potential applicability to the client's case.

### **Conclusion**

The question of whether a client should initiate a lawsuit for Internet defamation is one that requires careful consideration of the costs and risks. It is often extremely difficult to determine what a court will conclude is actionable "defamation" and what is protected "opinion." For example, a customer's opinions about his or her experience with a particular product, such as "this product is awful" are likely protected First Amendment speech that is not actionable. As we noted above, there are also serious potential costs to pursuing a potential defamation suit with significant risks to obtaining any meaningful recovery. Finally, the litigant must weigh the potential for reputational damage in the community tied to pursuing litigation, such as having to republish the harmful statements in court and in pleadings. See [www.](http://www.internetdefamationblog.com/category/case-results)

[internetdefamationblog.com/category/case-results](http://www.internetdefamationblog.com/category/case-results).

Faced with these significant barriers to suit, it is perhaps the best approach for counsel to first explore constructive pre-suit measures to resolve the dispute. In some cases, the client may be able to have the offensive commentary removed by sending a traditional cease-and-desist letter. Sending such a letter before initiating litigation may also have an added benefit of lending credibility to a claim that the defendant was acting in bad faith by refusing to remove the defaming commentary. See *Northern Light Tech., Inc. v. Northern Lights Club*, 236 F.3d 57, 65 (1st Cir. 2001) (affirming the district court's consideration of failure to remove content after receiving a cease-and-desist letter as a factor in the bad-faith determination). Of course, sending an inappropriate and over-the-top cease and desist letter could have the opposite effect. See *Green v. Fornario*, 486 F.3d 100 (3d Cir. 2007) (noting that an attorney who sent a cease-and-desist letter threatening criminal conduct for civil violations acted unwisely).

Nonetheless, if the client finds itself in the courthouse (whether to prosecute or defend), counsel is well advised to ensure that the client fully understands the risks as well as the potential rewards, the costs, and the potential for additional reputational damage so that the client's decision to litigate the issues is an informed one. ■

---

*Zachary G. Newman is a partner and Anthony Ellis is an associate with Hahn & Hessen, LLP, in New York, New York. Both are members of the firm's Litigation Practice Group. The authors thank Aaron Morris for providing some of the background material used to prepare this article.*