CORPORATE COUNSEL
An ALM Website
corpcounsel.com | February 17, 2017

Six Steps to Protecting Your Reputation Online

Should you litigate an online defamation? The answer depends on the circumstances and your overall goals.

Cliff Zatz, Joe Meadows and Laura Aradi

Credit: Pressmaster/Shutterstock.com

"A lie gets halfway around the world," it has been said, "before the truth can even pull its boots on." In today's world of online commentary and social media, this is truer than ever. Out of nowhere, you may be accused of poor service, selling defective goods, misleading customers, defrauding the government or committing other unethical or criminal conduct. These accusations may appear in e-mails to your clients, as posts on blog or review websites or in streamed videos on social media. What's more, they could be made or circulated by persons cloaked behind the anonymity of the internet. These fact patterns didn't exist 20 years ago, but internet defamation cases are now common, rapidly growing in the past five years. Here is a six-step guideline to handling them.

Understand the Basics of Defamation Law

Know the general elements of and defenses to a defamation claim. A plaintiff must establish that the statement is defamatory (provably false), concerns the plaintiff, was made by the defendant with some degree of fault (e.g., negligence or malice), was understood by the recipient and caused reputational or economic damage. In cases of defamation per se—accusations of criminal or unethical business conduct—damages may be presumed. A defendant can prevail by either negating any of the elements of the claim or showing that the statement is true.

These same elements and defenses apply when the defendant defamer is anonymous. In such a circumstance, the plaintiff faces additional obstacles: how to prove who made the statement, why and with what degree of fault. Proving defamation may depend on identifying and examining the defamer, who need not reveal his identity to assert defenses.

Assess Whether Action Is Necessary

Rule out inaction. Not every false statement is harmful, entitled to weight or likely to be seen by persons who matter. Perhaps the statement can be ignored because it lacks obvious credibility, appears in a low-profile internet location, will disappear on its own without threat of repetition or doesn't clearly target you.

Take Informal Action

Consider a counter-narrative to mitigate any damage. You might respond to the statement—in e-mails to clients or blog comments of your own—with your side of the story and call it a day.

Or you might use informal methods to take down the statement. First, ask or demand that the defamer retract the statement. In anonymous defamation cases, send the request through the same internet channels the defamer used to make the statement, or directly to the defamer if you can identify him. You may have leads on his identity based on the statement's content and timing or computer systems that track website visits or can trace e-mails. Second, ask the defamer's internet service provider (ISP), e-mail provider or the website hosting the defamatory statement (collectively, "mediums") to take down the statement. Mediums often have user policies, terms of service and content guidelines that prohibit obscene, threatening or unlawful statements, or the use of the medium's services to invade privacy interests or impersonate others. If the defamer has violated a medium's own rules, your request to take down the statement or for related action may be fruitful.

Identify the Goals and Risks of Litigation

In the end, litigation may be your best option. Before filing suit, identify your goals up front: Money damages? A retraction and injunction? "Victory" by default judgment? A strong message that you fight back to protect your name?

Evaluate the strength of your defamation claim and the risks of litigation. Common issues include:

- A short limitations period, often one year
- Whether the statement is one of fact (actionable) or opinion (not actionable)
- Meaning or "gist" of the statement to determine its truth or falsity
- Ease and cost of proving the statement's falsity
- Whether the plaintiff is a public figure, in which case malice must be shown
- Extent and availability of proof of reputational or economic injury
- Added evidentiary burdens in anonymous defamation cases
- Publicity surrounding the litigation
- The deterrent effect of the litigation on future defamers

The goals and litigation issues will drive your investment in the case.

Begin the Litigation

Draft your defamation complaint. Name the defendant defamer "John Doe" in anonymous cases unless you have enough facts and a good-faith basis to guess his real name. Using a real name could avoid a defense based on a First Amendment right to speak anonymously.

Consider other claims to bring and additional defendants to name. Defamation complaints sometimes include causes of action for false light, emotional distress, trademark or copyright infringement, unfair competition, tortious interference, fraud and invasion of privacy. They may also add as defendants those who worked in concert with or assisted the defamer (but not mediums: The Communications Decency Act generally immunizes them from tort claims arising out of defamation).

File your complaint, and in anonymous cases send out discovery subpoenas to mediums (or other third parties) for identifying information about the defamer. In some jurisdictions, either before or in conjunction with the filing of the complaint, you may seek early third-party discovery in the form of depositions or written discovery requests. You may also obtain an immediate hearing on whether you are entitled to identifying information about the defamer.

Discovery of ISP mediums is limited by law. Under the Stored Communications Act, ISPs may not produce user communications (emails). They may, however, produce user "record[s] or other information" such as a registered name, mailing address, phone number, secondary email address, internet protocol address and log-in and log-out dates and times. This information is vital to identifying an anonymous defamer. But often, the ISP has only the user's registered name and internet protocol address to produce. The name might be fake and the internet protocol address untraceable due to encryption or dynamic internet connections.

Litigate Aggressively

Prepare for immediate discovery fights, particularly in anonymous defamation cases. The medium may claim that a subpoena is overbroad or violates the Communications Decency Act or Stored Communications Act. The medium and the defamer (if appearing) may both claim that disclosure of defamer information violates anonymous speech rights under the First Amendment.

The First Amendment inquiry, if applicable, is complicated. Federal and state courts employ a variety of tests in deciding whether to order disclosure of information identifying an anonymous defamer. Typically, the tests require some notice of the claim to the defamer, prima facie proof of the underlying defamation and a legitimate need for the defamer's identity. In some jurisdictions, the test includes an extra step of balancing the competing interests—freedom from defamation versus freedom to speak anonymously.

Relevant facts in the First Amendment analysis include:

• Type of speech—political speech is protected more than commercial speech

• Method of speech—website posting is protected more than direct e-mailing

• Degree of malice—competitive motivations and hacking are less protected

• Expectation of privacy—defamer's efforts to maintain privacy weigh against disclosure

• Impact on other speakers—serious chilling effects weigh against disclosure

Most anonymous defamation cases fail when the plaintiff loses the First Amendment issue. The defamer remains masked, leaving the plaintiff unable to examine him about his fault in making the statement. In rare cases, the litigation has continued. There, the defamer's fault was shown through other evidence (e.g., continuing false statements during the litigation); could be shown using discovery methods that still shield the defamer's identity (e.g., telephonic depositions or depositions on written questions); or might be shown later and so the disclosure proceedings were continued.

Internet defamation cases—especially anonymous ones—are on the rise. A surprise cyber-defamation attack requires quick thinking and a game plan. Whether you can mitigate the damage informally or must elevate the matter to litigation depends on the strength of your case and the ultimate goals.

The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

Cliff Zatz *is a trial attorney and partner with Crowell & Moring LLP based in Washington, D.C., focusing on product liability, mass torts, cyber security and cases of emerging risks.* ***Joe Meadows*** *is a trial attorney and counsel with Crowell & Moring LLP based in Washington, D.C., focusing on complex litigation, internet defamation and expert evidence matters.* ***Laura Aradi*** *is an associate with Crowell & Moring LLP based in Washington, D.C., focusing on business torts, including internet defamation and employment disputes.*