Protecting Client Reputations In An Online World

By **Jim Wagstaffe**
July 25, 2018, 1:12 PM EDT


Jim Wagstaffe

You know it's the 21st century when you're contacted by a potential client and the described injury arises from an online perpetrator. Maybe it's defamation or bullying, or perhaps like in the recent case Herrick v. Grindr, it's "catfishing" — where someone impersonated the plaintiff and falsely reported them to be interested in meeting potential partners.[1]

There's no doubt we live in a world in which the internet has the potential to amplify defamatory communications unparalleled in human history. Plainly, the worldwide web vastly expands the reach and impact of online defamation, invasions of privacy, bullying and even revenge porn — all with the very real possibility that such cyberattacks are accessible in perpetuity. Ever increasingly, lawyers are playing a counseling and litigation role in protecting clients from the posting of negative information and reviews that otherwise might live on in the so-called blogosphere forever.

This changing world thus alters the traditional role of lawyers who heretofore were hired to write threatening demand letters and pursue lawsuits against the alleged perpetrators (and repeaters) of such informational wrongdoing. Today, the challenge becomes even identifying who are often anonymous online attackers, convincing internet service providers and websites to provide relief, and assisting clients in orchestrating reputation-preserving counter-attacks. Like Dorothy's admonition to Toto, we clearly are not in Kansas anymore for as has been said, Google is not simply a search engine — it's a reputation engine.

For the many early years of my career as a "media lawyer," I often provided clients with the soothing perspectives that today's newspaper is simply tomorrow's birdcage lining, that a good reputation will stand the test of the occasional private attacker, and justice could be found in the occasional lawsuit. However, protecting reputation and rights is ever so different in the online world of billions of google searches, ubiquitous Yelp reviews, countless cathartic websites for any and all aggrieved souls, and statutory immunity for the internet service providers, or ISPs, themselves.

The modern protective role played by lawyers in this internet communication free-for-all requires a completely different approach. First, the lawyer must help the client identify the alleged wrongful statements and determine whether their contextual placement online nevertheless is actionable at all. Second, the lawyer must understand Section 230 of the Communications Decency Act and determine the existence and scope of statutory immunities given to online communications. And finally, the lawyer must formulate a strategy — litigation and nonlitigation — to obtain removal or alteration of the damaging website materials.

The Legal Liability

The law of defamation is centuries old and premised on the deeply rooted notion that a person's good reputation is worthy of protection.[2] Importantly, the challenged statements must be false and defamatory, as statements of pure opinion are not actionable.[3]

When considering online defamation, courts often consider the context of the statements to determine if the readers understood them as actually being factual in nature. Perhaps ironically, the more hyperbolic or vituperative the website, the more likely it is that a judge could conclude that the statements do not declare or imply a provably false assertion of fact.[4]

In examining the context of online attacks, however, courts do not routinely conclude that they are the equivalent of "angry scrawls on bathroom walls."[5] Rather, false factual statements, especially if on a website that nominally requires the posting of accurate information, can still give rise to a successful libel suit.[6]

Section 230 Immunity

Section 230 of the Communications Decency Act provides that "[n]o 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."[7] This code section has widely been held to provide an immunity for websites that display third-party content. The prototypical cause of action for which the immunity attaches is one seeking to impose third-party liability for defamation.[8]

In addition, the section 230 protection is broader, providing immunity for liability premised to a wide range of publisher-related activity.[9]

The rationale is twofold: (1) that holding website operators liable for that content "would have an obvious chilling effect" in light of the difficulty of screening posts for potential issues; and (2) Congress sought to encourage websites to make efforts to screen content without fear of liability.[10] This hands-off approach comports with Congress's intention to permit the continued development of the internet with minimal regulatory interference.

There is one very recent break in the immunity chain: third-party liability for knowingly aiding and abetting sex trafficking. In what is called the Fight Online Sex Trafficking Act, or FOSTA, Congress just recently amended Section 230 to allow criminal and civil liability against online service providers who knowingly host third parties promoting or facilitating sex trafficking. Facing an onslaught of critical reaction, legislators and the president reacted to cases like Jane Doe No. 1 v. Backpage.com LLC where the court held that there was no website liability for allowing online "escort" advertising that facilitates sex trafficking.[11] Thus, many ISP's have reacted by closing down platforms for personals sites.

Lawyers can also assist their clients if they can show that if one can prove that the internet service provider itself materially contributed to the creation of the actionable content, then the immunity would not apply.[12]

Therefore, the lawyer's task is to separate the immunized sheep from the still-liable goats.

Generally, this will involve an awareness that the litigation approach will not work against the ISP's and as to them the only tools are persuasion and publicity. On the other hand, the originators of the online falsities, if discoverable, are still subject to litigation threats and filings. Here, however, the problems will be ones of identification (if anonymous) and enforcement.

There are still two major weapons in our modern litigation tool boxes. First, you can attempt to identify the anonymous poster through traditional investigation and, if unsuccessful, the filing of a Doe complaint followed by service of a subpoena on the ISP seeking identification.[13]

Second, while collecting a judgment against the often-impecunious poster may be problematic, more and more courts are allowing a post-judgment injunction against the defendant as to ongoing and future posts.[14] However, even here, be careful because some courts, citing Section 230, are limiting such relief to the individual defendant, and precluding an injunction that requires the ISP to take down the offending material.[15]

Strategies Lawyers Can Implement for Clients in a Modern Online World

Notwithstanding the broad protection for statements of opinion and Section 230's immunity, there are still five steps a lawyer can directly take for clients and five more they can take to assist their clients in implementing, addressing and possibly eliminating highly negative and false reviews.

Lawyer's Direct Steps

1. Contact the Sites: You can contact the site on behalf of your client and ask that the information be removed or corrected. To do this, you should locate the site's privacy policy and terms of use. In this current climate where sites like Facebook are proactively attempting to "clean up" their privacy and defamation hosting acts, you might well find a receptive audience for such removal efforts.

2. Directly Challenge the Anonymous Reviewers: An attorney can respond and even evaluate a defamation lawsuit against the actual posters of false reviews and comments. This can, as shown, include the filing of a "John Doe" lawsuit followed by a subpoena on the internet service provider to obtain the names and identifying information of the anonymous cyberattacker.

3. Litigate to Protect Your Client's Rights: The old-fashioned recourse to our court system to file defamation and related claims still exists as to the originators of the wrongful content. And, in some jurisdictions, you can even get a post-judgment injunction with the required teeth to take down the offending material.

4. Master the Algorithms: Lawyers must learn that many websites have algorithms and filters with characteristics that could more readily close off others' access to negative information about your client. For example, websites routinely place the most read reviews at the top of the page and have word identifiers to filter out, say, overly slanted

or undetailed reviews — learn these and help your clients.

5. Aggressively Fight Spoofing: When someone is impersonating your client or otherwise creating false webpages and sites in their name, take steps to stop such “spoofing” and obtain injunctive relief.

Recommend These Steps to Assist Your Clients

1. Examine Your Online Footprint: Regularly review your online profile — in other words, google yourself and regularly check online review websites like Yelp so as to identify what, if any, negative reviews are out there about you.

2. Respond: Consider posting a response to the negative review so that users can learn the true facts.

3. Encourage Positive Reviews: In the same vein, you can encourage those with positive views about your company or services to post and post often. Both by volume and location, this can decrease the negative impact of isolated bad reviews.

4. Create Content: The vast majority of internet users do not “drill down” past the front page or first page of reviews; therefore, the more searchable content you create about yourself, the more you can achieve the “burying” of the negative reviews and commentary.

5. Regularly Update Your Social Media Profiles: When someone is impersonating your client or otherwise creating false webpages and sites in their names, take steps to stop such spoofing such as obtaining injunctive relief. By regularly updating your social medial profile with positive descriptions, you can inoculate yourself at least partially against negative content out there.

In a world where there are tens of millions of google and website searches per minute, protecting one’s online reputation can be critical. Your reputation and perhaps your business could depend on it.

Jim Wagstaffe is the founder of The Wagstaffe Group, which recently released The Wagstaffe Group Practice Guide: Federal Civil Procedure Before Trial (LexisNexis, 2017). He is also a partner and co-founder of the law firm Kerr & Wagstaffe.

[1] See Herrick v. Grindr LLC (S.D.N.Y. 2018).

[2] Gertz v. Robert Welch Inc., 418 U.S. 323, 341 (1974) ("the individual's right to the protection of his own good name reflects no more than our basic concept of the essential dignity and worth of every human being—a concept at the root of any decent system of ordered liberty").

[3] Id.

[4] See Chaker v. Mateo (2012) 209 Cal. App. 4th 1138 (claim on opinion website that plaintiff was a "deadbeat dad" not actionable).

[5] ZL Technologies Inc. v. Does 1-7 (2017) 13 Cal. App. 603.

[6] Id.

[7] 47 U.S.C. sec. 230(c)(1)).

[8] Barnes v. Yahoo! Inc., 570 F.3d 1096 (9th Cir. 2009) (Yahoo! immune for failing to remove victim's ex-boyfriend's posting of fake online profiles); Jones v. Dirty World Entertainment Recordings, LLC, 755 F.3d 398 (6th Cir. 2014) (website not liable for uploaded defamation).

[9] See, e.g., Herrick v. Grindr LLC, 306 F.Supp.3d 579 (S.D.N.Y. 2018) (Grindr not liable for so-called "cat-fishing" claim where user impersonated plaintiff and falsely posted purported interest in fetishistic sex and bondage); Fields v. Twitter, Inc., 200 F.Supp.3d 954 (N.D. Cal. 2016) (Twitter not liable on theory it allowed ISIS to sign up for and use account that allegedly contributed to terrorist killings).

[10] Zeran v. America Online Inc. 129 F.3d 327, 331 (4th Cir. 1997).

[11] Jane Doe No. 1 v. Backpage.com LLC, 817 F.3d 12 (1st Cir. 2016).

[12] See Fair Housing Council of San Fernando Valley v. Roommates.com LLC, 521 F.3d 1157 (9th Cir. 2008) (online roommate service not immune from housing discrimination laws when it develops information about sex, family status and sexual orientation); FTC v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009) (no immunity for website that provided detailed information such as date, time and duration of telephone calls).

[13] See ZL Technologies Inc. v. Does 1-7 (2017) 13 Cal. App.5th 603 (court authorized subpoena against an otherwise immunized Glassdoor website because there was a prima facie showing of defamation against the fictitious defendants); see also Dendrite Int'l v. Doe, No. 3 (2001) 775 A.2d 756 (balancing required to allow disclosure of anonymous posters).

[14] See Balboa Island Village Inn Inc. v. Lemen (2007) 40 Cal. 4th 1141 (prior restraint doctrine does not prohibit post-judgment injunction).

[15] See Hassell v. Bird, California Supreme Court (July 2, 2018, No. S235968).