LexisNexis®

advancing what's possible

Protecting Reputation in an Online World

By Jim Wagstaffe, The Wagstaffe Group®

We live in a world in which the internet has the potential to amplify defamatory communications unparalleled in human history. Plainly, the World Wide 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 cyber attacks 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 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 counterattacks. 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 (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 lawyers 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 non-litigation—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. *Gertz v. Robert Welch, Inc.* (1974) 418 U.S. 323, 341 ("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"). Importantly, the challenged statements must be false and defamatory, as statements of pure opinion are not actionable. Id.

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

In examining the context of online attacks, however, courts do not routinely conclude that they are the equivalent of "angry scrawls on bathroom walls." *ZL Technologies, Inc. v. Does 1-7* (2017) 13 Cal. App. 603. 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. Id.

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." 47 U.S.C. sec. 230(c)(1)). 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. *Barnes v. Yahoo!, Inc.* (9th Cir. 2009) 570 F.3d 1096 (Yahoo!® immune for failing to remove victim's ex-boyfriend's posting of fake online profiles); *Jones v. Dirty World Entertainment Recordings, LLC* (6th Cir. 2014) 755 F.3d 398 (website not liable for uploaded defamation).

In addition, the section 230 protection is broader, providing immunity for liability premised on any publisher-related activity. See, e.g., *Jane Doe No. 1 v. Backpage.com*, LLC (1st Cir. 2016) 817 F.3d 12 (no website liability for allowing online "escort" advertising that facilitates sex trafficking); *Fields v. Twitter, Inc.* (N.D. Cal. 2016) 200 F.Supp.3d 954 (Twitter® not liable on theory it allowed ISIS to sign up for and use account that allegedly contributed to terrorist killings); 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).

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. *Zeran v. America Online, Inc.* 129 F.3d 327, 331 (4th Cir. 1997). This hands-off approach comports with Congress's intention to permit the continued development of the internet with minimal regulatory interference.

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

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 ISPs 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. 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).

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. See *Balboa Island Village Inn, Inc. v. Lemen* (2007) 40 Cal. 4th 1141 (prior restraint doctrine does not prohibit post-judgment injunction). 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. See *Hassell v. Bird*, California Supreme Court (July 2,2018, No. S235968).

Recommended Strategies for a Client in a Modern Online World

Notwithstanding the broad protection for statements of opinion and section 230's immunity, there are still several steps a lawyer can recommend that a client take (or you take on their behalf) to address and possibly eliminate highly negative and false reviews. My personal top 10 advice strategies are the following:

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. **Contact the Sites:** You can contact the site 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 very well find a receptive audience for such removal efforts.
4. **Create Content:** The vast majority of internet users do not "drill down" past the front page or front page reviews; therefore, the more searchable content you create about yourself, the more you can achieve the "burying" of the negative reviews and commentary.
5. **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.
6. **Regularly Update Your Social Media Profiles:** By regularly updating your social medial profile with positive descriptions, you can inoculate yourself at least partially against negative content out there.
7. **Know the Filters:** Many websites have algorithms and filters with characteristics that could more readily close off others' access to negative information about you. 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.
8. **Aggressively Fight Spoofing:** When someone is impersonating you or otherwise creating false webpages and sites in your name, you have rights to stop such "spoofing" and obtain injunctive relief.
9. **Consider Outing and Challenging the Anonymous Reviewers:** As shown prior, 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 cyber attacker.
10. **Litigate to Protect Your 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.

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.

About LexisNexis® Legal & Professional

LexisNexis Legal & Professional is a leading global provider of content and technology solutions that enable professionals in legal, corporate, tax, government, academic and non-profit organizations to make informed decisions and achieve better business outcomes. As a digital pioneer, the company was the first to bring legal and business information online with its Lexis® and Nexis® services. Today, LexisNexis Legal & Professional harnesses leading-edge technology and world-class content to help professionals work in faster, easier and more effective ways. Through close collaboration with its customers, the company ensures organizations can leverage its solutions to reduce risk, improve productivity, increase profitability and grow their business. LexisNexis Legal & Professional, which serves customers in more than 175 countries with 10,000 employees worldwide, is part of RELX Group, a world-leading provider of information and analytics for professional and business customers across industries.

LexisNexis®