Protecting Your Company’s Reputation on the Internet

Christopher J. Akin
Lynn Tillotson Pinker & Cox L.L.P.
Dallas

Ben Franklin once said that “It takes many good deeds to build a good reputation, but only one bad one to lose it.” While the Internet can be a powerful tool in enhancing a company’s reputation, it also is fertile ground for information that can damage, or in some cases even destroy, a company’s reputation.

How many times have you or your friends or colleagues gathered background information on a business or person by running an Internet search? Take the simple example of a local restaurant. In the past, a disappointed restaurant customer might have discussed the experience with friends and family – information that may well be harmful, but that, in and of itself, may not have a meaningful impact on the restaurant’s performance. But now that same person could post a message or comment on the Internet that would be available instantly to a global audience. If the message is posted on a popular website or blog, the restaurant critique might be viewed by a meaningful percentage of the restaurant’s potential customers, potentially persuading local residents, visiting businesspeople, and tourists not to visit the restaurant. The disgruntled customer might even post numerous messages under different user names, thereby creating the false impression that the restaurant has many unsatisfied customers.

Of course, every business assumes the risk of having one or more unsatisfied customers, but what if the negative review was posted by a disgruntled former employee or an unscrupulous competitor? And what if that disgruntled former employee or competitor also purchased meta tags from the most popular search engines, thus ensuring that the negative review appeared as one of the first search results for any search of the restaurant’s name on a major search engine?

While no company is immune from potential threats to its online reputation, the savviest companies will proactively identify potential threats, while also proactively taking steps to ensure that positive information about the company will be included in the first results for common internet searches about the company. This article discusses certain issues that companies frequently encounter in protecting their on-line reputations, such as issues commonly encountered under the Communications Decency Act, the Digital Millennium Copyright Act, and the Lanham Act. The article concludes with a discussion of how search engine optimization techniques may be used to proactively enhance a company’s on-line reputation.

For the uninitiated, it may be surprising to learn the extent to which an “interactive computer service” is protected against a potential claim of defamation. Congress passed the Communications Decency Act in 1996 with one of the stated goals of promoting unfettered speech on the Internet. The Act 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.1

Section 230 further provides that “[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.”2 In other words, the CDA “precludes courts from entertaining claims that would place a computer service provider in a publisher’s role,” and therefore bars “lawsuits 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.”3 Courts have frequently recognized that the CDA provides immunity to interactive websites for content created by a third party.4

The immunity conferred upon providers of an interactive computer service stands in stark contrast to the duties of traditional media providers. Indeed, it is well established that a traditional media provider such as a newspaper generally may not republish defamatory material.5 As a result, companies frequently will have a remedy for defamatory content published in a newspaper or magazine or reported by a television station. Except for articles or reports relying on anonymous sources, a traditional media provider generally will identify the speaker of a defamatory statement, thus providing the information necessary to identify the speaker in a potential lawsuit for defamation. Further, traditional media providers have the incentive to evaluate whether a proposed article contains defamatory content.

An interactive computer service does not have the same incentives as a traditional media provider. Consider the example of www.ripoffreport.com, an Internet message board that allows third party users to post and review complaints about businesses and individuals, without charge to the third party user. A user may create an account simply by providing a verifiable email address. To file a report, a user must complete three steps: (1) identify the name and address of the business or individual; (2) select a heading for the post, with options ranging from innocuous options to provocative options such as “ripoff” and “fraud”; and (3) draft the body of the report. It would be quite simple for a former employee or a competitor to make up a user name, provide a valid email address of someone else, and then post a defamatory report about the targeted business or individual. Unlike traditional media providers – which screen for defamatory content and frequently issue corrections for mistakes – Ripoffreport proudly touts that it has never removed a user posting. Reports posted on Ripoffreport often appear very high in the search results for Google and other major search engines. The reported cases involving the CDA highlight the difficulties of obtaining a finding of liability against an interactive computer service:
Barrett v. Rosenthal, 146 P.3d 510, 514, 528-29 (Cal. 2006) (CDA immunity applied even though site devoted to exposing health care frauds republished material after receiving warning that material was defamatory)

Zeran v. America Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) (holding that provider shielded from liability despite receiving notice of objectionable content on its website and failing to remove the disputed content)

Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.D.C. 1998) (finding interactive computer service provider immune from defamation liability for hosting gossip column, even though service provider paid gossip columnist compensation of $3000 per month, retained editorial rights, and promoted the columnist as a source of unverified gossip).

Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1102-03 (9th Cir. 2009) (Yahoo! had immunity for negligent undertaking claim based on failure to remove indecent profiles posted on its website by plaintiff’s former boyfriend).

While the CDA certainly creates challenges for businesses seeking to protect their reputations on the Internet, the challenges are not necessarily insurmountable. Indeed, the CDA does not provide immunity for content providers. A business therefore should examine very carefully whether a website that publishes defamatory content had any role in providing the disputed content. A potential area for exploration is whether interactive websites can be held liable for purchasing meta tags that result in allegedly defamatory postings by third-parties appearing higher in search results. Companies might also consider non-litigation approaches, such as taking proactive steps to create a positive Internet reputation that will result in negative information receiving less attention in Internet searches.

II. Lanham Act

The Lanham Act prohibits trademark infringement, trademark dilution, and false advertising, among other things. Of course, there are countless ways in which a company’s trademark rights might be violated on the Internet. For many companies, a common problem is the sale of the company’s products via third-party websites and on-line auctions in a way that either falsely suggests an affiliation with the company, or that results in the sale of expired, altered, damaged, or even counterfeit products. A perhaps extreme example was provided by the jeweler Tiffany’s, which once claimed that 73% of eBay listings for its jewelry were offering counterfeit products. Such problems can be difficult and expensive to police, given the large number of relatively small players selling products on-line, and the ability of violators to change user names and create new, infringing websites at minimal expense.

For companies dealing with such issues, it is important to understand the so-called first sale doctrine and its exceptions. Under the first sale doctrine, trademark law generally “does not reach the sale of genuine goods bearing a true mark even though the sale is not authorized by the mark owner,” meaning that “a distributor who resells trademarked goods without change is not liable for trademark infringement.” But the first sale doctrine does not protect sellers that create
a false impression of affiliation with the trademark owner. Nor does the first sale doctrine protect alleged infringers selling goods that are “materially” different from the goods sold by the trademark owner.

These exceptions to the first sale doctrine create the possibility for significant factual disputes about what is materially different and whether a website suggests a false affiliation with the trademark owner. For example, courts have held that the sale of expired products may raise a fact issue as to whether an alleged infringer is selling materially different products. Similarly, the question of whether a website or Internet advertisement improperly suggests an affiliation or endorsement also often is a highly fact-intensive issue. For many companies, there may be numerous potential targets for a trademark action, causing companies to weigh carefully the cost of legal action, the strength of a potential claim, and the financial impact of a failure to act.

III. The Digital Millennium Copyright Act

Companies seeking to protect their online reputations should also be familiar with the Digital Millennium Copyright Act of 1998 (“DMCA”). While copyright issues may not directly implicate a company’s online reputation, the conduct of an alleged infringer often implicates both trademark law and copyright law. Copyright law therefore may provide important leverage in resolving a dispute that directly impacts a company’s reputation. Moreover, because the DMCA’s notice and take down procedures have been used by some Internet service providers for non-copyright issues, it is helpful to understand that procedure and the obligations of Internet service providers. The DMCA consists of five titles and covers a variety of topics, but two particularly noteworthy provisions are the anti-circumvention provisions that prohibit attempts to circumvent technology designed to control access to a copyrighted work, and limitations on liability for copyright infringement by online service providers.

A. The DMCA’s Limitations on Liability for On-Line Service Providers.

Title II of the DMCA establishes four limitations on liability for copyright infringement by online service providers: (1) transient communications (acts of transmitting, routing or providing connections for the information, as well as the intermediate and transient copies that networks make automatically in their normal operation; (2) system caching (the practice of retaining information for a limited period of time so that subsequent requests for the same material can be satisfied by transmitting the retained copy, instead of retrieving a new copy); (3) storage of information residing on the service providers system at the direction of a user (including a notice and takedown procedure and a counter-notification procedural as a safeguard); and (4) information location tools (such as search engines, online directories, and hyperlinks).

The limitation on liability includes a complete bar on monetary damages, and a restriction on the availability of injunctive relief. To qualify for this protection, service providers must satisfy two general conditions: they must adopt and reasonably implement a policy of terminating accounts of repeat offenders, in appropriate circumstances, and they must accommodate and not interfere with “standard technical measures” for preventing copyright violations. There are also additional specific requirements for invoking the limitations on
liability. Some companies not only use the DMCA’s notice and take-down procedures for copyright issues, but also use them as a model for other types of take-down requests. Because companies almost inevitably will need to deal with on-line service providers, it is important to understand the rights and obligations of such providers.

B. The DMCA’s Anti-Circumvention Provisions

The DMCA provides that “[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title.” The DMCA’s anti-circumvention provisions have been somewhat controversial. A prominent example occurred in 2007, when internet users banded together to post and widely distribute a secret code used by the movie industry to prevent the piracy of high-definition movies. Initially, lawyers for the companies that use the copy protection system sent cease and desist to several websites that published the 32-digit code. Instead of complying with the request, “the legal notices sparked its proliferation on Web sites, in chat rooms, inside cleverly doctored digital photographs and on user-submitted news sites.” A musician even improvised a song in which he sang the code. The musician posted the song on YouTube, where it was played more than 45,000 times. The incident highlights the need for companies to consider carefully whom they want to pick a fight with and how to go about doing so. While the above example occurred in the context of anti-circumvention technology, companies face similar threats to their on-line reputations.

IV. Use of Search Engine Optimization Techniques

To protect their on-line reputations most effectively, companies should also consider using search engine optimization techniques to emphasize positive information and to de-emphasize negative information. In general, if a website appears earlier (or higher) in the search results for a popular search engine, a larger number of people will visit the website. Search engine optimization (“SEO”) involves the editing of a website so that it appears higher in search results on popular websites. In simple terms, a good SEO provider will make sure that a website includes relevant and commonly used search terms and has coding and other technical features that search engines rely upon.

SEO techniques are used frequently for a company’s own website, but many SEO providers can create positive content through affiliations with other existing websites. In some instances, companies may be able to create enough positive information to displace a site containing negative information, thus resulting in the negative information being harder to find. Consider the generic example of a company embroiled in controversial litigation, but with a chief executive officer and founder with a long-standing record of significant philanthropy. Without any action by the company, it is entirely possible that the first page of results for a Google search with the company’s name will return the company’s website and a series of links to sites with negative information about the pending litigation.

The founder’s philanthropic activities create an opportunity to change the playing field. An SEO provider might begin by creating links for press coverage and press releases of the founder’s philanthropic activities, and optimizing those links and possibly purchasing meta tags so that such positive links appear high in the search results for the company or its founder.
Certain SEO providers may have relationships with blogs and websites that generate substantial Internet traffic and perform well in Internet searches. Through those relationships, an SEO provider may be able to arrange for positive content about the founder’s philanthropic activities to appear in popular blogs and websites, thus creating additional positive content on the Internet. As the founder engages in new philanthropic activities, an SEO provider can continue to issue press releases and coordinate the creation of positive Internet content.

Ideally, a company should take steps to manage its on-line reputation before a problem occurs. One potential tactic to anticipate is that a litigation adversary may make aggressive claims in a lawsuit, and then purchase meta tags so that a link to the lawsuit appears at or near the top of the search results for the defendant company. Under many states’ law, there is a privilege against a defamation claim for statements made in a lawsuit, which means that a litigation adversary may face little or no potential downside as a result of such a tactic. The tactic will be less effective against a company that has taken proactive steps to maintain a positive reputation on the Internet.

A positive Internet reputation may have numerous other potential benefits. An obvious potential benefit is that the company may generate more revenue, but there are also less obvious benefits. As merely one example, The National Law Journal recently cautioned that trial attorneys should assume that some jurors will perform Internet research on the parties, notwithstanding the court’s instructions. Without condoning this practice, a company should prepare for the reality that its Internet reputation potentially could influence one or more jurors’ perception in any jury trial involving the company. Thus, a company’s investment in steps to maintain or create a positive on-line reputation should be considered as part of a long-term strategy to create business value and guard against potential future threats to the company’s reputation.

Christopher J. Akin
Lynn Tillotson Pinker & Cox L.L.P.
Dallas, Texas

4 See, e.g., Ben Ezra, Weinstein & Co. v. America Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123-24 (9th Cir. 2003); Morrison v. America Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000).
5 See Liberty Lobby, Inc. v. Dow Jones & Co., Inc., 838 F.2d 1287, 1289 (D.C. Cir. 1988). (“The common law of libel has long held that one who republishes a defamatory statement ‘adopts’ it as his own, and is liable in equal measure to the original defamer.”).
6 See Best Western Int'l, Inc. v. Furber, 2008 WL 4182827, at *10 (D. Ariz. Sept. 5, 2008) (no CDA immunity for statements that resulted from a collaborative effort); see also Fair Housing Council of San Fernando Valley v. Roommates.com, L.L.C., 521 F.3d 1157, 1164 (9th Cir. 2008) (CDA does not provide immunity for questionnaire used by roommate-matching website, when certain questions violated the Fair Housing Act); Barnes, 570 F.3d at 1109 (CDA immunity did not apply to promissory estoppel claim).
7 See Certain Approval Programs, L.L.C. v. Xcentric Ventures, L.L.C., 2009 WL 596582 (D. Ariz. Mar. 9, 2009) (denying motion to dismiss on basis of alleged immunity under CDA, where plaintiff had alleged that defendants
purchased meta tags that caused Internet searches for plaintiff’s names to show a title stating “Rip-off Report” before their names, among other allegations).


9 Polymer Technology Corp. v. Minran, 975 F.2d 58, 61-62 (2d Cir. 1992).

10 Scott Fetzer Co. v. House of Vacuums, Inc., 381 F.3d 477, 484 (5th Cir. 2004).

11 See Martin’s Herend Imports, Inc. v. Diamond & Gem Trading USA, Co., 112 F.3d 1296, 1302-03 (5th Cir. 1997).


14 Id.

15 Id.

16 Id.


19 Id.

20 Id.

21 Id.