Say What You Want: How Unfettered Freedom of Speech on the Internet Creates No Recourse for Those Victimized

Wes Gerrie

Follow this and additional works at: https://scholarship.law.edu/jlt

Part of the Communications Law Commons, First Amendment Commons, Internet Law Commons, and the Science and Technology Law Commons

Recommended Citation


This Article is brought to you for free and open access by CUA Law Scholarship Repository. It has been accepted for inclusion in Catholic University Journal of Law and Technology by an authorized editor of CUA Law Scholarship Repository. For more information, please contact edinger@law.edu.
SAY WHAT YOU WANT: HOW UNFETTERED FREEDOM OF SPEECH ON THE INTERNET CREATES NO RECOURSE FOR THOSE VICTIMIZED

Wes Gerrie*

“There are no saints online.”¹ This is a seemingly contemptuous statement about the Internet, a world-altering creation and revolutionary promise of a medium of mass communication, which has opened the global “marketplace of ideas” to all citizens.² It accomplished this by removing the gatekeepers of “old-world” media such as publishers, editors, and practical limits on immediacy and global reach.³ This “marketplace of ideas” is now open at all hours of the day and night, and any person with an internet connection can “become a town crier with a voice that resonates farther than it could from any soapbox.”⁴ At no time

---


² See Lyrissa Barnett Lidsky, Silencing John Doe: Defamation & Discourse in Cyberspace, 49 DUKE L.J. 855, 865, 893–94 (2000) (explaining the meaning and origin of the phrase “marketplace of ideas” as stemming from Supreme Court’s First Amendment Jurisprudence and encompassing the “sphere of discourse in which citizens can come together free from government interference or intervention”).


⁴ Reno v. Am. Civil Liberties Union, 521 U.S. 844, 870 (1997) (agreeing that Supreme Court precedent provides no basis for qualifying the level of First Amendment scrutiny that should be applied to the internet).
in history has the common man or woman held as much power as today. While the Internet spurred amazing innovation and revolution globally, it has also opened the door for new methods of harm and destruction.

It could be said that you do not put something online you would never say to your mother. Accompanying this saying is the impression that by posting something online that is negative, defamatory, or even false, causes serious repercussions. However, the reality is that this is simply not true. While technological advancements in the twenty-first century have increased the number of forums for individuals to anonymously vocalize in support of and against certain causes, one’s anonymity can be used as a weapon without there being any accountability in a court of law.

The news presents brazen accounts of psychological and emotional harm on celebrities or shocking tales of online dishonesty and negative schemes; however, the real harm for this lack of accountability and recourse occurs in large part because of the highly influential medium of online consumer

5 See Timothy J. D’Elia, Don’t Tread on Me . . . Online: The FEC Should Stay out of Free Internet-Based Political Speech, 24 CATH. U. J. L. & TECH 177, 177–78 (2015) (“The Internet has created an unparalleled forum for First Amendment expression, where any and all speakers can drive the marketplace of social ideas, opinions, and conscience.”).

6 See Patricia Sánchez Abril, Private Ordering: A Contractual Approach to Online Interpersonal Privacy, 45 WAKE FOREST L. REV. 689, 702 (2010) (“Digital disclosures are infinitely transferable, searchable, and permanent . . . Persons whose private information, images, or videos are digitally transmitted permanently lose control over that information and can never delete, defend, or rebut it—it simply becomes part of the permanent “Google-able” fabric of their reputation.”); Andy O’Donnell, 10 Things You Should Never Post on Social Networks, LIFEWIRE (June 5, 2017), https://www.lifewire.com/things-you-never-post-on-social-networks-2487415? (recommending that safe use the internet includes limiting the amount of personal information that is shared online because once personal information is shared, it is permanent).

7 See Information Is Permanent, iKEEPSAFE, http://archive.ikeepsafe.org/be-a-pro/reputation/information-is-permanent/ (last visited Dec. 19, 2017) (explaining how past online content can damage current interests). See also Christine Hauser, Yelp Reviews Cost a Yale Dean Her Position, N.Y. TIMES, June 22, 2017, at A25 (reporting how Yale Dean June Y. Chu lost her job as a result of posting Yelp reviews of local establishments that were “insensitive in matters related to class and race”); Brad Stone, Too Much Information? Hah! Sharing All Online Is The Point, N.Y. TIMES, Apr. 23, 2010, at A1, B7 (acknowledging that people are not considering the repercussions of sharing information online, and that there can be negative repercussions of doing so regardless of the content).

8 See Jeffrey R. Elkin, Cybersmears: The Next Generation, 10 BUS. L. TODAY 42, 44 (2001) (explaining how advocacy groups have worked with anonymous defendants to beat back defamation claims).

9 See Jonathan D. Glater, Judge Reverses His Order Disabling Web Site, N.Y. TIMES, Mar. 1, 2008, at A11 (quoting Judge Jeffrey S. White as he reversed his order that disabled the “Wikileaks” website on first amendment grounds, allowing banking customer’s personally identifiable information to be posted on the site again).
comments and reviews. Crowdsourced forums, such as online reviews, ratings, and comments – through sites such as Yelp, Google, and Amazon – are driving differentiation and have a powerful and lasting impact on everyday life. In the case of online reviews, in San Francisco, a half-star upgrade to a restaurant’s rating leads to an increase in the likelihood to sell out reservations. A similar situation can be seen in Seattle where a full star increase is equivalent to a “5-9 percent increase in revenue.” This influence has attracted great attention, especially given that people are more likely to share negative feelings than positive ones. For example, one study found that people are forty-five percent more likely to leave a negative review than a positive one.

See Andrew Bluebond, When the Customer Is Wrong, Defamation, Interactive Websites, and Immunity, 33 Rev. Litig. 679, 680 (2014) (“Elaborate tales involving celebrities expose wild stories of online dishonest and mean-spirited schemes, but much less discussed are the effects of untruthful and uncivil speech in the influential medium of online customer reviews of goods and services.”).

See generally Constance Gustke, A Bad Review is Forever: How to Counter Online Complaints, N.Y. Times, Dec. 10, 2015, at B9 (explaining how the number and quality of Yelp reviews can directly impact a business’s profitability, sustainability, and likelihood of closing); Chris Campbell, Catering to Shoppers? Know That Online Reviews Influence Them the Most, ReviewTrackers (Mar. 29, 2013), http://www.reviewtrackers.com/catering-shoppers-online-reviews-influence/ (explaining how online reviews influence 33 percent of online shoppers); see also Back to the Future – A Holiday Retail Story, Baynote, http://www.baynote.com/infographic/back-to-the-future/ (depicting graphic survey results that show online shoppers are most influenced by online ratings) (last visited Dec. 19, 2017); Conor Dougherty, Inside Yelp’s Fierce Google Grudge, N.Y. Times, July 2, 2017, at BU1, BU4 (detailing Yelp’s continuing antitrust actions against Google and explaining that Google Search results compete with Yelp, at times unfairly, driving differentiation). But see David Streitfeld, It’s Written in the Stars, N.Y. Times, June 9, 2016, at F2 (describing how a local New York restaurant encourages patrons to write outrageously unflattering Yelp reviews to effectively “opt out” from the review site).

See Michael Anderson & Jeremy Magruder, Learning from the Crowd: Regression Discontinuity Estimates of the Effects of an Online Review Database, 122 Econ. J. 957, 966 (2012) (explaining how comparing revenue data with Yelp review ratings demonstrates how impactful a half-star increase or decrease is on customer traffic).

See Michael Luca, Reviews, Reputation, and Revenue: The Case of Yelp.com 3–4, 6 (Harvard Bus. Sch., Working Paper No. 12-016), http://www.hbs.edu/faculty/Publication%20Files/12-016_a7e4a5a2-03f9-490d-b093-8f951238daba2.pdf (reviewing Seattle restaurant market revenue before and after the advent of Yelp, “a one-star increase leads to a 5-9 percent increase in revenue for independent restaurants, depending on the specification.”).

positive one. This truth is one-third basic psychology, one-third practicality, and one-third just down-right malicious intent. Yet despite the common axiom associated with its presumed repercussions, these types of negative, defamatory, and false online comments are becoming increasingly prevalent. Attempts to legally resolve negative, defamatory, and false online comments are unsuccessful.

Understanding this landscape, this Note discusses whether a user can truly say whatever they want on the Internet without legal recourse and, how that is possible. To start, Part I will provide the background of how free speech on the Internet has had limited recourse, discuss the technological developments that lead to companies like Yelp, and trace the growth of speech and consumer comments online. Part II will outline how Congressional acquiescence, recent legislation, and the Supreme Court has given interactive service providers immunity for any content published or uploaded by third-party users. Finally, Part III will demonstrate that there is binding precedent, federal and constitutional protections, and even legislation in the pipeline that gives users and consumers virtual autonomy when commenting and reviewing online. The result of these sections will prove that recent laws, media trends, and political objectives create an internet environment where the possibility of punishment for anything said online is essentially non-existent. In the end, this leaves businesses, victimized by negative, defamatory, and false comments and reviews, with little to no legal recourse or remedies.


17 A Survey of Customer Service from Mid-Size Companies, supra note 15 at 2 (reporting that more bad customer service stories are shared than good customer service stories).


19 See Maria Konnikova, The Psychology of Online Comments, New Yorker (Oct. 23, 2013), https://www.newyorker.com/tech/elements/the-psychology-of-online-comments (arguing that anonymity allows people to behave less civil than they would if it were known the online comment came from them); see also Campbell, supra note 11 (recognizing that negative reviews influence shopping habits).

20 See Glater, supra note 9 (describing Judge White’s frustration in his inability to curb online defamatory statements).
HISTORY AND BACKGROUND

Before diving into legal liability, a brief exploration of the complex world of interactive computer services and its users is necessary. Interactive computer services providers are websites on which individual users can create content and share information including comments, posts, ratings, and reviews.\(^{21}\) Some examples include: Twitter, Yelp, Amazon, UrbanSpoon, TripAdvisor, Angie List’s, and even the public pages of Facebook.\(^{22}\) Anyone with access to the Internet can read and use this content and information.\(^{23}\) One of the requirements for individuals conducting this content generation is merely that they provide a valid email address.\(^{24}\) The other requirement is that they choose a nickname to use when posting, creating anonymity, as these interactive service providers rarely require a legal name or residence.\(^{25}\) Despite this anonymity, the interactive service provider records the Internet Protocol (“IP”) address and stores it in its administrative database.\(^{26}\) Within minutes of becoming an actual customer of the business, a consumer can log onto the Internet, choose the interactive service

---

\(^{21}\) 47 U.S.C. §§ 230(f)(2)–(3) (2012) (defining an “interactive computer service” as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server” and an “information content provider” as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service”).

\(^{22}\) Brent A. Olson, Business Law Deskbook, ADVANCED TOPICS IN BUSINESS LAW §16B:82 CDA Immunity – “Interactive Computer Service” (2016) (acknowledging that courts have found MySpace, Facebook, Google, Amazon.com, and Yahoo! to be interactive computer service providers); Shelly Rosenfeld, The CDA as a Safe Harbor for Interactive Computer Service Providers, 36 L.A. LAW. 13, 13 (2013) (discussing Facebook, Twitter, Yahoo!, and Reddit as interactive computer service providers who hold immunity from third party postings which violate a law).

\(^{23}\) Paul F. Wellborn, III, “Undercover Teachers’ Beware: How that Fake Profile on Facebook Could Land You in the Pokey, 63 MERCER L. REV. 697, 698 (2012) (explaining how visitors may be able to see all, or a limited amount of content on the user’s page depending on the user’s profile settings).

\(^{24}\) Id. at 701-02 (discussing how social media websites require that you enter accurate and honest information during the registration process as well as noting that using the account with the purpose of projecting false information may be considered a criminal act). See also Brian Oltman, Agrimarketing in a Social Media World, 19 DRAKE J. AGRIC. L. 81, 87–89 (2014) (noting that in the agrimarketing field customers prefer testimonials which allow a person to be verified as a real individual and, under FTC regulations, require the disclosure of any compensation made in exchange for their review).

\(^{25}\) Laura Rogal, Anonymity in Social Media, 7 ARIZ. SUMMIT L. REV. 61, 62 (2013) (discussing how the internet requires an individual to create and utilize a nickname or “username,” rather than their legal name, and therefore promotes a culture of anonymity by excluding any identifying features).

\(^{26}\) Kristen L. Mix, Discovery of Social Media, 5 FED. CTX. L. REV. 119, 122 (2011) (explaining that while social media websites may have subpoena policies and protection under the Stored Communications Act, they are most likely retaining users’ photos, phone numbers, as well as their email, IP, and physical addresses).
provider of their choice, and review, comment and post about their experience for the world to see.\textsuperscript{27}

The sheer ease of use, accessibility, and availability has created an inherent value in this system. Yelp alone has an average of 88.6 million unique visitors covering 2.1 million businesses.\textsuperscript{28} In 2014, Yelp was responsible for 10,000 food orders a week based on its reviews.\textsuperscript{29} Additionally, ninety percent of shoppers will consider ten reviews or less before making a decision regarding a business.\textsuperscript{30} Consumers are exceedingly reliant on peers’ thoughts and comments on where to dine, shop, or visit, which makes maintaining a strong positive online presence of utmost importance.\textsuperscript{31}

Consequently, the massive volume of users and the ease of access that renders interactive service providers inherently valuable also leaves them ripe for abuse. Fifteen years ago, much of this innovation and connectivity with other consumers would have been impossible to achieve. However, its invention and

\textsuperscript{27} See also Khusbu Shrestha, \textit{50 Stats You Need to Know About Online Reviews [Infographic]}, VENDASTA (Aug. 29, 2016), https://www.vendasta.com/blog/50-stats-you-need-to-know-about-online-reviews#gs.Fm9B70Q (instructing potential clients on the importance of online reviews, including the fact that 44% of people want to consider reviews of purchases made within the last month); Abbey Stemler, \textit{Feedback Loop Failure: Implications for the Self-Regulation of the Sharing Economy}, 18 MINN. J. L. SCI. & TECH. 673, 704 (2017) (showing that instantaneous feedback tends to be more honest which may lower five star ratings for services, such as Airbnb).

\textsuperscript{28} Yelp.com, QUANTCAST, https://www.quantcast.com/yelp.com#trafficCard (last visited Dec. 19, 2017) (showing the average number of Yelp users for the U.S. and the rest of the world, as well as demographics (including age, race, income, gender, and education level) and individual interests (such as hobbies, food and drink, shopping, travel, and education and/or employment)).


\textsuperscript{30} \textit{Local Consumer Review Survey}, BRIGHTLOCAL, https://www.brightlocal.com/learn/local-consumer-review-survey/ (last visited Dec. 19, 2017) (examining how consumers make decisions on future purposes including how many times they need to visit a website, what factors they consider the most in reviews, and how many rating pages they will visit prior to finalizing their choice).

\textsuperscript{31} Marti Trewe, \textit{When customers threaten to post negative Yelp reviews}, AM. GENIUS (May 30, 2012), https://theamerican genius.com/real-estate-coaching-tutorials/when-customers-threaten-to-post-negative-yelp-reviews/ (discussing the importance of maintaining such a positive reputation through reviews has resulted in people threatening to post poor reviews and discredit the candidate otherwise).
proliferation has opened the floodgates of new methods of damage and mischief.\textsuperscript{32} This type of misuse has created an avalanche of litigation regarding negative content individual users create on interactive service providers.\textsuperscript{33} Accordingly, when a business sees a comment online they feel could impact their business because it is fraudulent, defamatory, or maliciously negative, their first instinct is to seek legal action against the interactive service provider itself.\textsuperscript{34}

**INTERACTIVE SERVICE PROVIDER IMMUNITY**

There are numerous legal theories under which businesses could assert claims against online sites which host negative, defamatory, and even fake online reviews and comments.\textsuperscript{35} This avalanche of potential legal claims includes defamation, fraud, libel, false light, and hate speech to name a few.\textsuperscript{36} These

\begin{itemize}
\item \textsuperscript{32} Noam Cohen & Brian Stelter, *Airstrike Video Brings Attention to Whistle-Blower Site*, N.Y. Times, Apr. 7, 2010, at A8 (illustrating that we live in an online world where people can post things without accountability, exemplified by WikiLeaks). See also Bailey Roese, *Defamation, Humiliation and Lost Reputations: Mitigating the Damage to Women Harassed Online*, 35 WOMEN’S RTS. L. REP. 123, 123-25 (2014) (showing how women may be targeted online with humiliating and defamatory posts which are made to undermine them but with little recourse).
\item \textsuperscript{33} Andy Radhakant & Matthew Diskin, *How Social Media Are Transforming Litigation*, 30 GPSOLO 74, 74 (2013) (discussing how the increase in social media has caused an increase in the variance of types of lawsuits which are being brought, but there are also new ethical concerns that need to be taken into consideration for all parties, including the judge and jurors).
\item \textsuperscript{34} L. David Russell, Christopher C. Chiou, & Zain A. Shirazi, *Fake It Until You Make It? Battling Fake Online Reviews*, LAW360 (June 9, 2014, 12:17 PM), https://www.law360.com/articles/545366/fake-it-until-you-make-it-battling-fake-online-reviews (discussing how if there is defamatory post that one is looking to remedy, they should first go to the third-party poster, and if no change is done, they must then file a lawsuit, they will not, however, be able to recover from a host service under CDA immunity).
\item \textsuperscript{35} See Constance Gustke, *A Bad Review is Forever: How to Counter Online Complaints*, N.Y. Times, Dec. 10, 2015, at B9 (acknowledging that an exception to Yelp’s policy that an entity may not remove negative reviews “is when someone violates content guidelines through hate speech or by not having had the experience they’re actually reviewing”); Eleanor Vaida Gerhards, *Your Store Is Gross! How Recent Cases, the FTC, and State Consumer Protection Laws Can Impact a Franchise System’s Response to Negative, Defamatory, or Fake Online Reviews*, 34 FRANCHISE L.J. 503, 504 (2015) (discussing that while there are multiple avenues to bring a lawsuit against the host website where the negative review is posted, these are generally unsuccessful due to immunity under the Federal Communications Decency Act); Lucille M. Ponte, *Protecting Brand Image or Gaming the System: Consumer Gag Contracts in an Age of Crowdsourced Ratings and Reviews*, 7 WM. & MARY BUS. L. REV. 59, 67 (2016) (noting that plaintiffs have tried to recover for poor reviews posted online under multiple legal theories, including a new growing concept which only allows consumers to post positive reviews).
\item \textsuperscript{36} Jonathan Bailey, *5 Easy Ways to Get Sued on Facebook*, PLAGIARISMTODAY (Aug. 25, 2010), https://www.plagiarismtoday.com/2010/08/25/5-easy-ways-to-get-sued-on-
theories are fairly broad, ranging from unfair competition to civil extortion.\textsuperscript{37} Despite the vast array of available legal theories, businesses face insurmountable hurdles in holding these sites responsible for defamation and rarely, if ever, succeed in litigation against online review sites.

A. Communications Decency Act

The most prevalent and overwhelming of these articles is the Communications Decency Act ("CDA"). Congress passed the CDA in 1996 as a crucial tool to protect freedom of expression and innovation on the Internet.\textsuperscript{38} In reality, the CDA was originally an attempt by Congress to regulate pornographic material facebook/. Five of the primary ways to be sued for a comment on social media include: (1) libel, an untrue matter which harms an individual’s reputation (2) copyright infringement, posting something without the original creator’s permission (3) privacy, where one posts a matter which infringes another’s right to privacy (4) breach of contract, primarily violations of a non-disclosure agreement, and (5) harassment, the continuous behavior of being intrusive on another. Id.; see also Torati v. Hodak, 147 A.D.3d 502, 503-04 (2017) (finding that posts that were made to the general public were not actionable as libel because they were deemed to be only an opinion, but direct messages made through social media were actionable); Gattoni v. Tibi, LLC, 2017 WL 2313882, at *1–2 (S.D.N.Y. May 25, 2017) (holding that where a copyright pending photograph posted on Instagram is cropped and reposted without the copyright designation by another party, the plaintiff must show (1) the work which was allegedly stolen, (2) that they are the rightful owner, (3) that the copyright has been properly registered, and (4) how and when the defendant violated the copyright claim); Chaney v. Fayette Cty. Pub. Sch. Dist., 977 F. Supp. 2d 1308, 1315 (2013) (noting that where a student voluntarily posted a picture of themselves in a bikini on their social media page with the privacy settings visible to friends and friends of friends, they relinquished a right to claim privacy because they had no control over who the friends of friends were); Cummins v. Bat World Sanctuary, 2015 WL 1641144, at *26–27 (Apr. 9, 2015) (holding that in an action for defamation, because the appellant published statements with actual malice they were defamatory, and in an action for breach of contract, the contract terms must be expressly violated for there to be sufficient evidence of the breach); Piester v. Escobar, 36 N.E.3d 344, 346, 348 (2015) (holding that comments made on social media and established evidence of stalking were considered harassment and therefore not protected by the First Amendment).

Gerhards, supra note 35 at 504 (showing the broad stretch of lawsuits which can be brought for defamatory remarks, but explaining that under the CDA of 1996, a suit cannot be brought against an interactive computer service provider if immunity requirements are met); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122 (9th Cir. 2003) (identifying a broad list of complaints, including but not limited to invasion of privacy, misappropriation of the right to publicity, defamation, and negligence and holding that the plaintiff could not recover on any of her claims because of host website immunity rules under the CDA).

Robert Cannon, The Legislative History of Senator Exon’s Communications Decency Act: Regulating Barbarians on the Information Superhighway, 49 FED. COMM. L.J. 51, 78 (1996) (analyzing the CDA as needing to be reviewed with strict scrutiny, and arguing that it must not create undue regulations which would “reduce the adult population . . . to . . . only what is fit for children”).
on the Internet by restricting indecency and obscenity in cyberspace. However, in *Reno v. American Civil Liberties Union*, the Supreme Court struck down the anti-indecency portions of the CDA. The only surviving section is section 230, a response to the New York state opinion in *Stratton Oakmont v. Prodigy Services* where an online message board operator was subjected to liability for defamatory posts by its third party users. Following this decision, Congress enacted section 230, also known as the Communications Decency Act, as a piece of sweeping legislation to give courts the ability to dismiss such suits against interactive service providers on grants of immunity and privilege.

**Textual Analysis**

Section 230 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.” Congress’ goal was “to promote the continued development of the Internet...[and] to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive

---

39. Id. at 64 (discussing how Senator Exon’s influential technique of showing the “Blue Book” of pornography proved influential by educating other members about what was available for anyone to find on the internet and swayed those on the fence to vote against pornography to protect their reputations); see also Jay Alan Sekulow & James Matthew Henderson, Jr., *Unsafe at any [Modem] Speed: Indecent Communications Via Computer and the Communications Decency Act of 1996*, 1 U. F.L.A. J. TECH. & POL’Y 1, 48–59 (1996) (discussing the debate in Congress on the meaning of “indecency” and how it was considered in conjunction with First Amendment rights, leading to a change in the proposed legislation).

40. *Reno*, 521 U.S. at 875–76 (determining that the government did not meet its burden in showing that it was not narrowly tailored enough to meet the compelling government interest of keeping children safe); see also Sable Communities of Cal., Inc. v. FCC, 492 U.S. 115, 129–30 (1989) (discussing how it is helpful in determining when a communications based restriction is narrowly tailored if there is a strong legislative history to show that no other reasonable alternatives existed).

41. See 47 U.S.C. § 230(c)(1)–(2) (2012) (creating a standard that an interactive computer service provider will be treated as a publisher and therefore not responsible for third party comments); accord Bluebond, supra note 10 at 689 (discussing how Stratton Oakmont v. Prodigy Services heavily influenced Congress’ decision to pass section 230 of the CDA which would provide immunity for the interactive computer service providers when a third party posts a comment which infringes on the rights of another).

42. Charles D. Tobin, *Indecent Attacks on the Communications Decency Act?*, 41 LITIG. 8, 8 (2015) (stating that Congress passed legislation which would prohibit a plaintiff from filing a lawsuit against an interactive computer source provider, when a third party is responsible for the tort); Heather Saint, *Section 230 of the Communications Decency Act: The True Culprit of Internet Defamation*, 36 Loy. L.A. ENT. L. Rev. 39, 45–46 (2015) (noting that while Section 230 grants immunity to almost all websites which allow for comments as they are not the author, this prevents the victim of the defamatory remarks from being able to recover as the actual poster may be unknown due to the anonymous atmosphere of web message boards).

computer services.”\textsuperscript{44} The two critical terms are “interactive computer service” and “information content provider.” The former captures interactive service providers that provide or enable access, basically any online service that publishes third-party content, and the latter captures the users and creators of content and information on these services.\textsuperscript{45} Because section 230(c)(1) guarantees that interactive service providers will not be treated as publishers, section 230(c)(2)(A) protects them from liability for “any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.”\textsuperscript{46} Thus, section 230 is an immunity that provides a shield for interactive service providers to use against potential liability for any communication by their users.\textsuperscript{47} Effectively, the CDA decimated the aforementioned theoretical universe of numerous legal theories that create liability.\textsuperscript{48}

\textit{Judicial Interpretation}

The following cases will demonstrate that Courts have interpreted the CDA broadly to immunize almost all interactive service providers from libel actions stemming from third-party content. The Fourth Circuit in \textit{Zeran v. America Online} was the first to endorse and support this broad view stating that Congress granted outright immunity.\textsuperscript{49} Even more recent cases attempting to circumvent the CDA show that legal recourse through the court system is futile.\textsuperscript{50} For

\begin{itemize}
\item \textsuperscript{44} Id. U.S.C. §§ 230(b)(1)–(2).
\item \textsuperscript{45} Id. § 230(f)(2)–(3); see generally Miree Kim, \textit{Narrowing the Definition of an Interactive Service Provider Under § 230 of the Communications Decency Act}, INTELL. PROP. & TECH. F. AT BOS. C. L. SCH. (Mar. 31, 2003), http://bciptf.org/?p=242 (explaining the definitions of both an interactive computer service and an information content provider).
\item \textsuperscript{46} See 47 U.S.C. § 230(c)(1)–(c)(2)(A).
\item \textsuperscript{47} See generally Les Machado, \textit{Immunity for Interactive Computer Service Providers Under Section 230 of the Communications Act for Information Originating from Third Parties}, NIXON PEA BODY, LLP (Jan. 6, 2005), http://www.nixonpeabody.com/116747 (explaining the three subparts of Section 230 that provide the shield against potential liability); Bluebond, supra note 10 at 692 (discussing how broad the immunity shield is that has become less clear in its interpretation since 2014); Gerhards, supra note 35 at 504 (discussing how large of an umbrella is case by Section 230 and some examples of what is protected such as trade libel, slander, invasion of privacy, etc.).
\item \textsuperscript{48} See Bluebond, supra note 10 at 691.
\item \textsuperscript{49} Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (holding that through Congress grants outright immunity through Section 230 “to any cause of action that would make service providers liable for information originating with a third-party user of service.”).
\item \textsuperscript{50} See generally Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1165, 1177 (9th Cir. 2007) (holding that Google’s hyperlinking and use of thumbnails as part of an image search was a fair use of Perfect 10’s images because it was “highly transformative”); Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1118 (W.D. Wash. 2004)
\end{itemize}
example, Amazon has successfully invoked the CDA immunity over the past decade to avoid liability for third-party product reviews and posts in virtually all of its lawsuits.\textsuperscript{51} Broad judicial interpretation has allowed the CDA to overlay most state tort laws to protect interactive website operators from being subjected to publisher liability.\textsuperscript{52} This insulates them from responsibility for their users’ statements whether they are unfair, defamatory, extortive, or even fraudulent.\textsuperscript{53}

Courts across the country have shut down even the smallest of windows for imposing liability through their broad interpretation of the CDA.\textsuperscript{54} For example, the only small and narrow window the courts left ajar is in situations in which the interactive service provider has collected user-generated posts and manipulated the posts for the website because this could approach content creation under the CDA.\textsuperscript{55} This type of issue seems like a possible exception under the CDA.\textsuperscript{56} However, this narrow exception relies on the courts considering whether the edits substantially transcended editorial control, which would not be sufficient for content creation.\textsuperscript{57} More often than not the courts have found such an action to be in the domain of editorial control – a key element of publishing that is directly under the umbrella of CDA immunity.\textsuperscript{58} Thus, courts have extended CDA’s immunity provision to editorial acts such as decisions on whether to publish, withdraw, postpone, or edit things like users’ comments and members’ posts.\textsuperscript{59}

(holding that Amazon is protected from liability on its third party platform which allows vendors to post products to sell themselves); Schneider v. Amazon.com, Inc., 31 P.3d 37, 41 (Wash. App. Ct. 2001) (ruling in favor of Amazon because the CDA does not immunize contract claims, so all claims were dismissed and Amazon is found to be protected from any liability).

\textsuperscript{51} See generally Perfect 10, Inc., 508 F.3d at 1176; Corbis, 351 F.Supp.2d at 1118; Schneider, 31 P.3d at 40.

\textsuperscript{52} Les Machado, Immunity for Interactive Computer Service Providers Under Section 230 of the Communications Act for Information Originating from Third Parties, Nixon Peabody, LLP (Jan. 6, 2005), http://www.nixonpeabody.com/116747; Bluebond, supra note 10 at 681.

\textsuperscript{53} Id.

\textsuperscript{54} Id. at 684.

\textsuperscript{55} Id. at 694–95.

\textsuperscript{56} See, e.g., id. at 700 (acknowledging that although this may seem like a broad exception to CDA immunity, it is not).

\textsuperscript{57} Id. at 694–96 (discussing the consideration courts will give regarding internet site editorial conduct and looking to precedent to see factors those courts have considered in editorial liability cases); Gerhards, supra note 35 at 505–06 (stating that “the CDA provides a nearly airtight defense to prevent a franchise from successfully suing an online review site for false or defamatory content in a third-party review.”).

\textsuperscript{58} Bluebond, supra note 10 at 694–96; e.g. Levitt v. Yelp! Inc., No. C-10-1321, 2011 WL 5079526, at *6–9 (N.D. Cal. 2011).

\textsuperscript{59} Id. at 695–96; see generally Gerhards, supra note 35 at 505–06 (discussing cases that have extended the CDA’s immunity provisions).
The legal protections the CDA provides are unique to U.S. law because the vast majority of countries do not have similar protections. While these countries are technologically advanced and have similar levels of internet access, most prominent interactive service providers are based in the United States. The attraction for these businesses is that the CDA renders the U.S. a safe haven and thus favorable legal environment for websites that want to provide a platform for their users to post virtually anything.

B. Prevalent and Recent Lawsuits Against Interactive Service Providers

Many controversial and highly publicized lawsuits against interactive service providers have pushed out the boundaries of CDA immunity. Since its passing in 1996, lawsuits involving the CDA have attempted to push the boundaries of immunity and have forced courts to provide guidance on how far the immunity extends. As noted above, the courts have interpreted the CDA extremely broadly and recent lawsuits have demonstrated that standard.

In *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC.*, the Ninth Circuit held that Congress’ intent was minimal interference with online speech even if the concern was “creating a lawless man’s land.” There, the operator of a roommate-matching website, which required users to answer questions about gender and sexual-orientation, was liable because they were no longer an interactive service provider passively transmitting information; it was a content creator. Thus, the court determined that immunity should only be denied if a website requires discriminatory content, such that

---

61 Id.
63 See Bluebond, supra note 10 at 692.
65 See Bluebond, supra note 10 at 694–96 (explaining how the court in Levitt v. Yelp! ruled that removal of certain content is immunized as something publishers do, and Section 230(c)(1) protects service providers from publisher liability); see also Gerhards, supra note 35 at 506 (showing that the court treats these issues broadly by dismissing a claim against Yelp for “economic extortion because the business had no right to positive reviews under any agreement [...] or under any law.”).
66 *Fair Housing Coun. of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1164 (9th Cir. 2008).*
67 Id. at 1161–62.
allowing or even encouraging defamatory content is permissible.\textsuperscript{68} Even the dissent given in \textit{Roommates.com} believed the legal environment on the matter should be changed; however, a strong and deferential immunity exists.\textsuperscript{69}

More recently, in \textit{Levitt v. Yelp!}, the Ninth Circuit recognized that even if an interactive service provider like Yelp manipulated and created negative online content, those allegations would be “entirely speculative” and blocked by the CDA.\textsuperscript{70} In this case, small business owners alleged that Yelp extorted advertising payments from small businesses by manipulating user reviews to be negative until they paid.\textsuperscript{71} Ultimately, the court found no liability as even practices of unfair competition like coercing advertising in exchange for more limited negative content online is the “traditional editorial function of a publisher” and thus evokes CDA immunity.\textsuperscript{72} The court eventually held that plaintiffs have no pre-existing right to positive content, nor do interactive service providers have the obligation to provide them.\textsuperscript{73}

Recently, one of the key decisions that could undermine the CDA slightly was overturned and reversed by the Sixth Circuit. In \textit{Jones v. Dirty World Entertainment}, Nik Richie, on his website thedirty.com, encouraged and commented on third-party information that Jones, a high-school teacher and Cincinnati Bengal cheerleader, was a “freak” and slept with “every Bengal Football Player.”\textsuperscript{74} The trial court found that by encouraging and commenting on slanderous information, he had invalidated any CDA immunity.\textsuperscript{75} However, the Sixth Circuit reversed, rejecting the “encouragement test,”\textsuperscript{76} and held that an interactive computer service provider that adds commentary to allegedly tortious third-party content does not thereby preclude its CDA immunity.\textsuperscript{77}

\begin{flushright}
\textsuperscript{68} \textit{Id.} at 1171; see S.C. v. Dirty World, LLC., No.11-CV-00392-DW, 2012 WL 3335284, at *4 (W.D. Mo. Mar. 12, 2012) (stating that “merely encouraging defamatory posts is not sufficient to defeat CDA immunity”).
\textsuperscript{69} \textit{Fair Hous. Coun. of San Fernando Valley v. Roommates.com, LLC,} 521 F.3d 1157, 1171 n.15, 1177 (9th Cir. 2008) (McKeown, J., dissenting).
\textsuperscript{70} \textit{Levitt v. Yelp! Inc.,} 765 F.3d 1123, 1129 (9th Cir. 2014).
\textsuperscript{71} \textit{Id.} at 1133.
\textsuperscript{72} \textit{See id.} at 1130–32; \textit{Seaton v. TripAdvisor, LLC,} 728 F.3d 592, 595 (6th Cir. 2013) (surmising even inappropriate procedure like using an “improper method” and/or using known “unverifiable data” is protected by the CDA).
\textsuperscript{73} \textit{Levitt,} 765 F.3d at 1133.
\textsuperscript{74} \textit{Jones v. Dirty World Ent. Recordings, LLC,} 965 F.Supp.2d 818, 823 (E.D. Ky. 2013).
\textsuperscript{75} \textit{Id.} at 821.
\textsuperscript{76} \textit{Jones v. Dirty World Ent. Recordings, LLC,} 755 F.3d 398, 415 (6th Cir. 2014). See Christine N. Walz & Robert L. Rogers III, \textit{Sixth’s Circuit’s Decision in Jones v. Dirty World Entertainment Recordings LLC Repairs Damage to Communications Decency Act}, 30 ABA COMM. LAW. 4, 5 (Sept. 2014) (recognizing that under the “encouragement test,” a website operator could lose immunity merely by inviting (i.e. encouraging) authors to post potentially defamatory so they may add their own editorial comments).
\textsuperscript{77} \textit{Jones,} 755 F.3d at 415.
\end{flushright}
Finally, the Second Circuit had the most recent crack at CDA immunity and gave it the broadest reading to date. In *Ricci v. Teamsters Union Local*, the court held that a plaintiff defamed online may attempt to sue the original speaker, but may not sue the messenger. The Second Circuit was in full consensus on this holding. Additionally, the court created a growing and non-exhaustive list of internet service providers that are, categorically, immunized such as social networking sites, MySpace, Craigslist, and now, GoDaddy.

In short, the CDA provides a nearly airtight defense to prevent a business from successfully suing an interactive service provider for false, defamatory, or overly negative posts in a third-party comment. Therefore, because the CDA provides immunity, plaintiffs must find an alternative method for redress—perhaps the posters of the content themselves.

**USER AND CONSUMER AUTONOMY**

Congress and the courts have determined that interactive service providers are to have full immunity. Nonetheless, they have left open the small possibility that those who post content the website did not explicitly create could be subject to liability. However, a user’s anonymity, sweeping state legislation, feasibility and practicality, and upcoming federal actions provide insurmountable legal

---

78 *See, e.g.*, *Ricci v. Teamsters Union Local*, 781 F.3d 25, 28 (2d Cir. 2015)  (showing other circuits have created an ongoing list of internet-based service providers and the second circuit would be adding GoDaddy to that list).

79 *Id.*

80 *Id.*

81 *Id.* (citations omitted).

82 *See* Janine Eccleston, *Can You Be Sued If You Give A Bad Review On Yelp?*, INVESTOPEDIA (Jan. 14, 2013, 2:00 AM), https://www.investopedia.com/financial-edge/0113/can-you-be-sued-if-you-give-a-bad-review-on-yelp.aspx (showing that lawyers who represent these cases advise writer of these reviews to only post about opinions and truths, and if they don’t lie or misrepresent yourself you should not be held liable).

83 *See id.* (suggesting that because Yelp encourages its users to be honest about their reviews and cautions users to omit excessive exaggeration that the users could be the ones potentially held liable one day).

84 *See Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1124 (9th Cir. 2003) (stating that “under § 230(c), [...] so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process.”).

hurdles. Together, these hurdles create their own protection and have given the online user virtual autonomy.

A. Anonymity

“Anonymity has a long history in American discourse,” having been established as protected under the First Amendment. This was explicitly outlined in McIntyre v. Ohio Elections Commission, which stated that an author’s anonymity was an aspect of freedom of speech protected by the First Amendment and exemplified by the framers. Three years later, the Supreme Court expanded this protection in Reno v. American Civil Liberties Union, holding online speech should enjoy the same anonymous speech protections as traditional forms of media. Despite this policy, free speech and the right to speak anonymously is not absolute and a plaintiff has the right to seek redress for harmful anonymous speech under defamation. This is much easier said than done.

To remain anonymous, online posters and commenters use a variety of tactics to protect themselves from even the smallest chance of liability. They start with the most tried and true method of staying anonymous for which the devious have used for centuries – fake names – however, in this case they use fake usernames as well. Next, during the registration process, they use temporary email addresses, commonly known as ‘disposable email addresses,’ to create a new email address that keeps their real name and real email address away from the interactive service provider. They do this while on “Virtual Private

87 See generally id.
90 Reno, 521 U.S. at 885.
91 Lively, supra note 88 at 697 (2015); but see McIntyre, 514 U.S. at 357.
92 See generally Andy Greenberg, How to Anonymize Everything You Do Online, WIRED (June 17, 2014, 6:30 AM), https://www.wired.com/2014/06/be-anonymous-online/ (discussing several ways to become anonymous online).
Networks” that hide the users IP address and “run all online data via a secure and encrypted virtual tunnel” that prevents identification. Short of destroying all technology and living in a cave immediately after posting, the combination of these methods allow users to remain anonymous and post online without any real risk.

Because a user’s identity is unknown, the plaintiff would have to file a lawsuit against an anonymous “Doe” defendant. However, in this Internet age when an anonymous statement is made, courts have required identification of the defendant to determine if statements are indeed defamatory for liability to amass. As a result, a large number of defamation, fraud, and malice lawsuits against the user have centered on requested identification of anonymous online posters. For identification to occur and once the complaint has been filed against “Doe,” the plaintiff then gets the opportunity to serve a subpoena on the interactive service provider to “unmask” the user. This is when anonymity becomes contentious as those interactive service providers will fight tooth and nail to save their user’s identifying information.

Unmasking Statutes

Courts must balance First Amendment rights of the potential defendant against the right to assert a claim, when trying to determine whether or not to reveal an anonymous poster’s identity. Consequently, lawyers, judges, legislators, and scholars have struggled to define the limits of anonymity in the Internet Age. Nevertheless, around 2000 a consensus standard began to

---

95 Drew Prindle, How to Stay Anonymous Online, DIGITAL TRENDS (May 16, 2013, 10:31 AM), https://www.digitaltrends.com/computing/how-to-be-anonymous-online/ (showing how VPNs can anonymize your location and mask your IP address).
96 Tufnell, supra note 94.
97 See generally Greenberg, supra note 92.
98 Lively, supra note 88 at 700; see generally Russell et al., supra note 34 (noting how subpoenaing an anonymous user’s identity is difficult).
101 Lively, supra note 88 at 700; see generally Russell et al., supra note 34 (discussing the current legal landscape on how difficult it may be to find anonymous posters’ identities).
102 See generally Russell et al., supra note 34.
103 Lively, supra note 88 at 700; see generally Russell et al., supra note 34 (explaining the difficulties in gaining a poster’s identity); In re Cohen, 887 N.Y.S.2d at 429 (recognizing the need to balance an individual’s “right to communicate anonymously” with being held responsible for “abusing [ing] the opportunities presented by [the Internet]”).
emerge after the court in *Dendrite International, Inc. v. Doe* articulated a four-part test to deal with a defamation case involving anonymous speakers on online message boards. The burden is on the plaintiff to provide: 1) notice of the subpoena and sufficient time for a response; 2) proof of the exact statements at issue; 3) an evidentiary showing on the merits of the claim; and 4) a necessity for disclosure of Doe’s identity. The *Dendrite* standard already imposed a high burden on the plaintiff, and since then, the standard for unmasking has only increased. In *Doe v. Cahill*, the court modified the third criterion to clarify that the plaintiff must make a prima facie case for each element of the defamation claim. Thus, courts now require the plaintiff to produce sufficient evidence supporting each element of its cause of action. Finally, *Independent Newspaper, Inc. v. Brodie* further tightened the standard by instructing courts to require all of the criteria to be satisfied; the prima facie case must be strong, akin to a summary judgment standard.

**Unmasking Application**

By tightening the standard, courts expressed concern with a potential “sue first, ask questions later approach” with a relaxed standard and minimal anonymity protection. Therefore, the standard has become very difficult to meet, especially in its application. First, providing notice and ample opportunity to respond may seem simple enough; however, the nature of an

---


105 *Dendrite Int’l*, Inc., 775 A.2d at 767–68. The Dendrite standard has become the express and formal standard in the District of Columbia and nine states including Connecticut, Texas, Arizona, Indiana, Maryland, New Hampshire, Pennsylvania, Illinois, and Wisconsin, and according to a Westlaw search conducted in December 2017, has been cited in more than 70 cases across the country. Paul Alan Levy, *Developments in Dendrite*, 14 Fla. Coastal L. Rev. 1, 12–13 (2012).

106 *Dendrite Int’l*, Inc., 775 A.2d at 767-68.

107 *See* Doe v. Cahill, 884 A.2d 451, 464 (Del. 2005) (upgrading the burden on the plaintiff to prove a prima facie case for each element); Shepard & Belmas, *supra* note 104 at 109–11.

108 *Cahill*, 884 A.2d at 457.

109 *Id.* at 463.


111 Shepard & Belmas, *supra* note 104 at 109 (citing *Cahill*, 884 A.2d at 457).

112 *See* *Cahill*, 884 A.2d at 464 ("[W]ithout discovery of the defendant’s identity, satisfying this element may be difficult, if not impossible.").
anonymous defendant is that they are hard to find and defendants may not possess the financial or temporal resources to meet this criterion.113 Second, on its face, it may seem easy to provide the exact alleged defamatory statements, but sometimes a plaintiff is unable to get subsequent access because, in the fast-paced, constantly changing environment of the Internet, a specific post can easily get lost in the shuffle or deleted.114 The third element is the criteria which has been heightened the most since Dendrite.115 In most unmasking cases, the plaintiff has failed to provide sufficient evidence of harm and has not proven each element to a sufficient degree, especially with subsequent cases trending in favor of a tighter standard.116 Lastly, the balancing test under the fourth criteria serves only to tilt the scales in favor of protecting anonymous speech, as even a viable defamation claim can be dismissed when comparing to long-held, historical, and binding constitutional interests.117 The lens which this is viewed through is the belief that “[a]nonymity makes public discussion more uninhibited, robust, and wide-open” values prevalent in American jurisprudence.118 To conclude, plaintiffs must first navigate the complex labyrinth of anonymity and unmasking before they can even proceed with proving their case.

B. Lawsuits Against Users – The Individual

If a plaintiff successfully navigates the murky waters of unmasking the defendant, a plaintiff can now file suit – but that by no means is the end of a plaintiff’s hurdles.

Anti-SLAPP

Laws against the Strategic Lawsuit Against Public Participation (“Anti-SLAPP” statutes) are designed to prevent lawsuits intended to censor, intimidate, and silence critics by implementing financial burdens on litigation

113 See Indep. Newspaper, Inc., 966 A.2d at 450 (“[T]he plaintiff must undertake efforts to notify the anonymous poster that he is the subject of a subpoena or application for order of disclosure”); Lyrissa Barnett Lidsky, Anonymity in Cyberspace: What Can We Learn from John Doe?, 50 B.C. L. Rev., 1373, 1374 (“[F]ew [people] had the resources to find counsel and file motions to quash.”).

114 Shepard & Belmas, supra note 104 at 108.

115 See Lidsky, supra note 113 at 1378–89; Shepard & Belmas, supra note 104 at 109.


117 Lidsky, supra note 113 at 1380.

118 Id. at 1383.
until they abandon their opposition. An Anti-SLAPP statute has a favorable effect on critics by removing impediments on their freedom of speech. Twenty-eight states and the District of Columbia have passed similar statutes and have become more prevalent. Anti-SLAPPs vary slightly from state to state, but generally they permit a defendant to dismiss a complaint, especially one of defamation, “early in a case and recover attorneys’ fees and costs.”

In order for a defendant facing an Anti-SLAPP motion to prevail, they “must show that the statement in question 1) was made in a public forum, 2) concerned an issue of public interest, and 3) that plaintiff is not likely to succeed on the merits of the claim.” Generally, online posts are categorically held to be “statements in a public forum.” In addition, courts generally hold that the statements, especially online reviews, concern an issue of public interest. This fact is particularly difficult for plaintiffs because it expands the traditional definition of an issue of public interest. The last prong is the one that is particularly quarrelsome. Although the burden of proving Anti-SLAPP is on the defendant, in reality it is onerous on those bringing the defamation suit because it requires them to provide proof of success of their claim. This entails, by clear and convincing evidence under the totality of the circumstances, proving all the elements can be satisfied, which means the plaintiff may have to prove its case before some of the evidence can even be properly obtained.

Anti-SLAPP concerns are just another consideration for defendant’s filing suit against an online user. Plaintiffs must carefully assess – spending time and money – their case or else a court will not only dismiss the case but order the payment of fees and costs to the defendant. Additionally, the presence of an

120 See Nina Golden, *Slapp Down: The Use (and Abuse) of Anti-SLAPP Motions to Strike*, 12 RUTGERS J.L. & PUB. POL’Y 426, 426 (2015); Quinlan, supra note 119 at 368.
121 Gerhards, supra note 35 at 510 (referring to Arizona, Arkansas, California, Delaware, District of Columbia, Florida, Georgia, Hawaii, Illinois, Indiana, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Missouri, Nevada, New Mexico, New York, Oklahoma, Oregon, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Vermont, and Washington).
122 Russell et al., supra note 34.
123 Russell et al., supra note 34 (citing Wong v. Jing, 117 Cal. Rptr. 3d 747, 759 (Cal. Ct. App. 2010)).
124 Id.; e.g. Wong, 117 Cal. Rptr. 3d at 760.
125 Gerhards, supra note 35 at 510.
126 Id.
127 Russell et al., supra note 34.
129 See e.g., id. (“Defendants are awarded attorney fees and costs on appeal, the amounts of which are to be determined by the trial court on demand.”).
Anti-SLAPP statute in their state may alone be enough to entirely dissuade a company from filing suit in the first place.  

**Defamation**

The final hurdle is proving the defamation cause of action itself. Defamation law is often difficult for courts to apply online due to the large number of people involved, anonymity in posting, and the frequently changing nature of the Internet. To prevail on a cause of action of defamation, the plaintiff has the burden of showing: 1) a false and defamatory statement of fact; 2) to an unprivileged third party; 3) of and concerning the plaintiff; 4) with the requisite degree of fault; 5) which produces harm.

Elements one, two, three, and four are often easy to establish because of the inherent characteristics of the action. Because the unmasking identifies the user, the user’s post is published on the Internet for all to see, satisfying element two. The post must be, in some way, derogatory and about the plaintiff or else the cause of action would be moot and unnecessary for the victim to undertake fulfilling elements one and three. Finally, constitutional concerns established in Anti-SLAPP determine the requisite degree of fault — element four. Consequently, by substantiating these elements plaintiffs must prove the remaining two elements: the statement made was of fact and the statement was harmful in nature, which in most cases, is difficult to prove.

To have liability under a claim of defamation, the statement in question must be understood to be fact. The statement’s truthfulness is not a dispositive

---


131 See generally Alison E. Horton, Beyond Control?: The Rise and Fall of Defamation Regulation on the Internet, 43 VAL. U. L. REV. 1265, 1296 (2009), http://scholar.valpo.edu/cgi/viewcontent.cgi?article=1122&context=vulr (addressing the complexities associated with applying libel law to the Internet).

132 See Bluebond, supra note 10 at 686-87.

133 See id.

134 See id. at 686.

135 See generally id. at 688 (2014) (“The first element requires that the statement be defamatory as a matter of law.”).

136 See id. at 687-88.

137 See Man Threatened with Defamation Lawsuit Over Negative Yelp Review, CBS N.Y. (Mar. 21, 2014, 7:19 PM), http/newyork.cbslocal.com/2014/03/21/man-threatened-with-defamation-lawsuit-over-negative-yelp-review/ (recognizing Law Professor Leon Friedman’s assessment that challenges facing plaintiffs in libel cases are that they must prove something was both false and ruined someone’s reputation).

138 See Sommer v. Gabor, 48 Cal. Rptr. 2d 235, 248–49 (Cal. Ct. App. 1996) (emphasizing that statement in question must be understood as fact); see generally Costanza
factor; the user must merely communicate it to be factual.\textsuperscript{139} Under this rationale, opinions are too subjective to be considered a statement of fact and are privileged under the law.\textsuperscript{140} Thus, the burden is on the plaintiff to prove the review or comment is not an opinion and rises to the level of being understood as a fact.\textsuperscript{141} To determine this distinction, the factors that a court will balance include:

- (1) whether the specific language in issue has a precise meaning which is readily understood;
- (2) whether the statements are capable of being proven true or false;
- and (3) whether either the full context of the communication in which the statement appears or the broader social context and surrounding circumstances are such as to signal . . . readers or listeners that what is being read or heard is likely to be opinion, not fact.\textsuperscript{142}

This balancing requirement mandates that the plaintiff prove the meaning of the statement was to provide information and to prove the statement itself is false – both difficult especially if the post has some validity.\textsuperscript{143} Context can swing either way depending on the court, as some judges will consider review sites to contain mostly opinions and some will find them as a source of important information.\textsuperscript{144} There is a strong possibility that a court will find a review or post online to be an opinion and therefore not covered under defamation.\textsuperscript{145}

The closing element of defamation is a showing of harm.\textsuperscript{146} Rather than proving specific losses, individuals making a defamation claim may recover by proving a harm to their reputation.\textsuperscript{147} Businesses are not entitled to a presumption of harm because they do not necessarily have a personal reputation.
or the ability to feel hurt or embarrassment. Instead, a business must show the statement in question is directly traceable to a tangible, adverse loss on their business operations. The adverse loss element requires the plaintiff to create and prove a causal link between the particular post and an impact on their business. This involves a preponderance of the evidence, which is difficult to obtain, like direct admission, witness testimony, and high levels of access to the review. Adverse loss also requires a showing of financial records that can be both awkward to divulge and inconclusive in their traceability to the post. For these reasons, it will be challenging for a business to show that an online post had the requisite harm for a defamation claim.

C. Speak Free Act

More hurdles will come in the future due to political action. In addition to the hurdle of the relevant state law, there is currently a great deal of pressure on Congress to strengthen freedom of speech protection. The Speak Free Act is a bipartisan initiative Congress introduced on May 13, 2015, by Republican Blake Farenthold from Texas and Democrat Anna Eshoo from California. The technology lobby, free speech advocates, and notably, Yelp, proposed the

---

148 Bluebond, supra note 10 at 687 (2014) (“[B]usinesses do not have personal reputations, hurt feelings, or embarrassment that would entitle them to presumed damages.”).
150 Richie, 544 N.W.2d at 25; Flaks v. Koegel, 504 F.2d 702, 706–07 (2d Cir. 1974).
151 See generally Gerhards, supra note 35 at 509; see Richie, 544 N.W.2d at 25 (acknowledging that harm can be proven by direct evidence); see also Flaks, 504 F.2d at 707 (exemplifying that a causal link is simply that the damages flow from the wrongdoing).
bill. Its purpose is to be equivalent to a federal Anti-SLAPP statute, intended to curtail legal threats over online reviews. The Act allows anybody who reviews or comments on a good or service online to file a special motion to protest the claim. The judge would then rule on the motion potentially dismissing the case with prejudice, meaning the defendant could not only recoup legal fees and costs, but could also potentially acquire damages of their own. The policy is to protect and encourage critical open dialogue, especially online on a blog or a consumer review site. If this act were to pass, it would provide a huge deterrent on a national scale to businesses seeking recourse for false, defamatory, or malicious posts online. Currently, the act has been co-sponsored by twenty Democrats and twelve Republicans, and fifty-nine of the top legal scholars in the United States.

D. Practical and Emotional Limits

Even if one is somehow able to get through this gauntlet facing potential plaintiffs and develop a strong case, there are some very real and very practical limitations on a business seeking redress. As in all areas of operating a business, it is ultimately an extremely difficult balance to control the potential risk to brand image, reputation, and credibility seeking redress for disparaging online comments and reviews.

Therefore, another reason potential defendants should look before leaping into litigation is negative publicity. If a business sues an online user, it is very easy for that individual user to pit public opinion against the business, creating a “David versus Goliath” situation. For example, in New York, a customer gave

---

161 Id.
164 Id.
166 Russell et al., supra note 34 (showing the difficulty in fake reviews and proving a plaintiff’s case to get redress).
167 Id.
168 Man Threatened with Defamation Lawsuit Over Negative Yelp Review, supra note 137.
169 Id.
a two-star review on Yelp to Ron Gordon Watch Repair.\(^{170}\) The shop filed a petition for defamation and the user subsequently posted the notice letter on his Facebook page.\(^{171}\) Almost immediately, Gawker and other media sites picked up on the post, garnering over 110,000 views and numerous negative reviews due to the potential litigation, not his business.\(^{172}\) As illustrated by Ron Gordon Watch Repair, the publicity of litigation will likely give the review more recognition and promotion than it otherwise would have received had it been left unfettered.\(^{173}\) The principle here is that even strong claims may have serious repercussions due to an aggressive stance in responding to an online user.\(^{174}\)

Moreover, even if the lawsuit is successful, the plaintiff is more likely to find judgment-proof defendants than those with deep pockets.\(^{175}\) Libel law gives successful plaintiffs compensatory and occasionally punitive damages, remedies that are worthless when the defendant has no money to satisfy a judgment.\(^{176}\) Vindication for successfully proving falsity can only go so far without marketing the legal victory and the absence of a “take-down” remedy for the offending post.\(^{177}\) This further enhances the potential “David versus Goliath” dichotomy and could potentially alienate the business in the online community.\(^{178}\)

In attempts to level the playing field, many businesses have tried to use “non-disparagement clauses” in consumer sales agreements.\(^{179}\) The idea behind these provisions is to prevent negative reviews at the outset and restrict any negative impacts on reputation, products, services, management, or employees.\(^{180}\) These inconspicuous clauses on receipts, invoices, or customer sale contracts have been harshly criticized as being “bad business,” but could act as a deterrent of

\(^{170}\) Id.


\(^{172}\) Biddle, supra note 171.


\(^{175}\) Bluebond, supra note 10 at 683.

\(^{176}\) Lidsky, supra note 113 at 1389-90.

\(^{177}\) Id. at 1390.

\(^{178}\) Id. at 1374.


negative posts. Most non-disparagement clauses are found to be unenforceable – precluded by the First Amendment right to free speech.

To conclude, while it is true that a business may have an outside chance of bringing a successful suit against an individual online user, there exist significant hurdles which may outweigh any potential remedies. The legal hurdles along with the with the risk of damage to the business’s brand and reputation, work against any potential remedies assuming the recourse is even available and feasible in the first place.

CONCLUSION

The Internet has made good on its original promise of revolution and has changed the world forever. However, because it is largely unregulated – or at the very least drastically under-regulated – it has become the modern-day “Wild West.” The Internet can be a harsh and unforgiving forum for even the most respected brands and products. Regardless of their size, social media and the global online community have made companies more vulnerable to negative online attention. This negative attention can be in the form of libel, extortion, or fraud, all of which produce no remedies under the current legal environment.

Nowadays, consumers rely heavily on what they read on the Internet, rendering every customer a potential reviewer and a potential problem for business. The dissatisfied can easily reach interested audiences over a panoply of media. This reality has shifted not only the economic strength from business owners and traditional media to the consumers, but also the legal balance as well. These shifts are visible in the immunity interactive service

182 Herb Weisbaum, Yes, You Can Post That Negative Online Review, Says Congress, NBC NEWS (Dec. 7 2016, 11:17 AM), https://www.nbcnews.com/business/consumer/yes-you-can-post-negative-online-review-says-congress-n693001; see also, CAL. CIT. CODE § 1670.8 (West 2015). State legislators such as those in California have enacted laws to prevent non-disparagement clauses. CAL. CIT. CODE § 1670.5 (West 2015). Additionally, the Consumer Review Fairness Act of 2016 was passed December 14, 2016 which prohibits companies from putting disparagement clauses in consumer contracts that prevent customers from making statements about the company’s products, services, or employees.
183 Gerhards, supra note 35 at 503–04.
184 Bluebond, supra note 10 at 680.
185 Id. at 680.
186 Gerhards, supra note 35 at 504.
187 Bluebond, supra note 10 at 682; Campbell, supra note 11.
188 Bluebond, supra note 10 at 682.
189 Id. at 682.
providers have and are reflected in the minute probability that a plaintiff business can successfully sue individual consumers and users posting online.\textsuperscript{190} While businesses are forbidden from shooting the messenger, the original sender is safeguarded and thereby permitted to continue acting without repercussion.\textsuperscript{191}

In conclusion, for those participating in the global online community worried about the harms caused by “cyber smears,” the current state of the law is dispiriting.\textsuperscript{192} Any mischievous bandit can start a campaign of lies, defamation, and libel that leaves their victim with no meaningful recourse.\textsuperscript{193} The twenty-first century’s “Wild West” is a relatively unstable, under-regulated, and unfiltered frontier which has been innovative and profitable for some, but devoid of legal remedies for most.\textsuperscript{194} Under the current legal framework, the old adage you can “say whatever you want” on the Internet will inevitably continue to be true.\textsuperscript{195}

\textsuperscript{190} Id. at 684.
\textsuperscript{191} Id. at 684 n.14.
\textsuperscript{193} Id.
\textsuperscript{194} Gerhards, \textit{supra} note 35 at 503-04.
\textsuperscript{195} Elkin, \textit{supra} note 192 at 47.