LOSING THEIR LICENSE TO LIBEL: REVISITING § 230 IMMUNITY

Vanessa S. Browne-Barbour

ABSTRACT

Libel, an ancient tort, protects one's reputation in a community. Historically, libel damages were presumed because of the tort's potential to cause permanent reputational harm. Today, the likelihood of such reputational harm is increased exponentially by the prevalence of the Internet, where billions of pages of information are accessible to more than two billion people. When libel occurs on the Internet, why should the law favor the interests of Internet service providers (ISPs) over the interests of the libeled? In applying § 230 of the Communications Decency Act (CDA) to defamation claims against ISPs arising from defamatory statements on ISP sites, the overwhelming majority of courts follow the lead of the United States Court of Appeals for the Fourth Circuit and decline to hold ISPs accountable for the tort of libel, along with other civil and criminal claims. This overly broad interpretation of § 230 essentially renders a well-established cause of action a nullity. Why should a statute designed to protect ISPs from liability for blocking or restricting access to pornography or other objectionable materials be construed to bar defamation claims, even when the ISPs have not engaged in conduct to limit access to offensive materials?

This Article argues that courts should adopt a narrower interpretation of § 230 to allow a remedy for defamation. Alternatively, it argues that Congress should adopt the DMCA as a model in revising § 230 by incorporating notice and take-down provisions. Such notice and take-down provisions would permit state common law defamation claims against ISPs, assuming the ISPs had actual or constructive knowledge of the defamatory content and failed to remove it within a statutorily mandated time period. Distributor or secondary publisher liability based on actual or constructive knowledge is consistent with traditional defamation law.
I.  INTRODUCTION ................................................................. 1506

II.  HISTORICAL VIEWPOINTS .................................................. 1508
    A.  HISTORY OF DEFAMATION ............................................. 1508
    B.  MAKING OF THE CDA & LEGISLATIVE HISTORY ................... 1518

III.  SECTION 230 .................................................................. 1523
    A.  CONTENTS OF § 230 ..................................................... 1523
    B.  LEGISLATIVE HISTORY OF THE CDA ............................... 1525
    C.  JUDICIAL INTERPRETATION OF § 230 ............................... 1527
        1.  CDA Immunity from Defamation Upheld .......................... 1528
        2.  CDA Immunity Defense Does Not Apply .......................... 1538

IV.  PROPOSED CHANGES ......................................................... 1546
    A.  DIGITAL MILLENNIAL COPYRIGHT ACT (DMCA) ................... 1546
    B.  COURTS SHOULD CONSTRUE THE CDA MORE NARROWLY ........ 1551
    C.  CONGRESS SHOULD REVISE § 230 OF THE CDA ................... 1553
    D.  INTERNATIONAL LAW AND ONLINE DEFAMATION .................. 1556

V.  CONCLUSION .................................................................. 1559

I.  INTRODUCTION

In light of states’ historical authority to provide a remedy to their citizens for reputational harm, one would think that individuals should be able to recover for defamatory statements made online about them, especially given society’s increased reliance on email, online news sites, online editorial columns, interactive websites, blogs, and various forms of social media for the daily communication of information.\(^1\) Online

---

\(^1\) See generally Joshua Azriel & Charles Mayo, In The Age Of Social Media, Times v. Sullivan and Gertz v. Welch Decisions Still Important to Defamation Trials, J. INTERNET L., Feb. 2014, at 26 (commenting that increased use of various forms of social media “increases the likelihood that someone’s reputation may be harmed”); see also Susan Freiwald, Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation, 14 HARV. J.L. & TECH, 569, 584 (2001) (suggesting that “serious online defamation presents more than just an academic question and its incidence will likely accelerate as cyberspace communications become even more widespread”); Reno v. ACLU, 521 U.S. 844, 853 (1997) (commenting that the Internet “constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers”).
defamation presents a serious public policy problem in light of its potential to cause significant harm to its victims’ reputations.² Yet courts to date have generally barred individual defamation and related state common law claims against Internet Service Providers and other interactive computer services (collectively referred to herein as ISPs).³ They have done so based upon an overly broad interpretation of § 230 of the Communications Decency Act of 1996 (CDA).⁴ Congress enacted § 230 to immunize ISPs from liability for limiting or restricting online access to pornography, obscenities, and other objectionable materials.⁵ Courts have extended that immunity to other federal and state law claims as well.⁶ This Article argues that Congress should revise § 230 of the CDA by incorporating a notice-based safe harbor provision modeled after the Digital Millennium Copyright Act (DMCA). Such a revision would impose liability on ISPs for third-party defamatory content only on proof of notice and subsequent failure to remove the defamatory content within a reasonable time. A revised § 230 would spare courts the current quandary of granting nearly blanket immunity to ISPs that have notice of material, and would incentivize ISP self-regulation, as the original Act intended.

Part II of this Article explains the history and current status of defamation law generally. This Part also examines two cases that provided the backdrop to which the drafters of the CDA responded. Part III discusses the content of the CDA, surveys the legislative history of the CDA, and concludes with a review of the subsequent jurisprudence

² Freiwald, supra note 1, at 584; see also PROSSER AND KEETON ON TORTS § 113, at 799 (W. Page Keeton et al. eds., 5th ed. 1984) (noting that “the last utterance may do no less harm than the first”).

³ Robert L. Rogers III, Ninth Circuit Court of Appeals Holds That Communications Decency Act Does Not Bar Actions Against Website Operators For Failure To Warn, 31 COMM. L. 8, 8 (2015).

⁴ At 47 U.S.C. § 230(f)(2) (2012), the CDA defines 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, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.” Internet websites are the most common types of interactive computer services. Id.; Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157, 1162 n.6 (9th Cir. 2008). Although the U.S. Supreme Court has found other portions of the CDA unconstitutional, § 230 survives. Id. at 1162 n.5.

⁵ See, e.g., Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1101 (9th Cir. 2009) (noting that some of the “sister circuits have recognized, Congress enacted the Amendment in part to respond to a New York state court decision”) (citing Roommates.com, 521 F.3d at 1163); Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

⁶ See infra Section III.C.1.
relating to § 230 of the CDA and its effect on the ability of individuals to recover damages from ISPs for online defamatory content posted by third parties. Part IV proposes changes to the CDA and discusses the safe harbor provisions of the DMCA,7 which could serve as a model for the revision of § 230 of the CDA. Incorporating notice and take-down provisions modeled after the DMCA would permit state common law defamation claims against ISPs, assuming the ISPs had actual or constructive knowledge of the defamatory content and failed to remove it within a statutorily mandated time period. Such liability based on actual or constructive knowledge is consistent with traditional defamation law.8 Alternatively, Part IV further argues that an unamended § 230 of the CDA should be interpreted to allow private plaintiffs to seek redress from ISPs when defamatory content is posted on their websites by third parties. It recommends that courts adopt a narrower interpretation of the scope of the CDA to allow such relief. The Article concludes by asserting that, under either theory, the application of § 230 of the CDA should follow the traditional defamation law model, which imposes liability on distributors or secondary publishers who communicate information with actual or constructive knowledge of the defamatory content.9

II. HISTORICAL VIEWPOINTS
A. HISTORY OF DEFAMATION

Libel and slander compose the two basic forms of defamation.10 The Restatement (Second) of Torts defines libel as “the publication of defamatory matter by written or printed words, by its embodiment in physical form or by any other form of communication that has the potentially harmful qualities characteristic of written or printed words.”11 In contrast, slander results from “the publication of defamatory matter by spoken words, transitory gestures or by any form of communication other

---

7. Digital Millennium Copyright Act, 17 U.S.C. § 512 (2012) (providing a safe harbor for online service providers to limit liability for unauthorized use of copyrighted materials); see also Lucille A. Jewel, You’re Doing It Wrong: How the Anti-Law School Scam Blogging Movement Can Shape the Legal Profession, 12 MINN. J.L. SCI. & TECH. 239, 240 (2011) (commenting that CDA immunity encourages “critical ideas and arguments; a different system, such as a notice and take-down scheme,” as in the DMCA likely would result in a “less robust exchange of ideas”).
9. Id.
11. Id. § 568(1).
than those stated in” the preceding definition for libel.\textsuperscript{12} Additionally, a defendant may be held liable for slander per se when the defamatory statements include an accusation of crimes of moral turpitude,\textsuperscript{13} loathsome disease,\textsuperscript{14} or serious sexual misconduct.\textsuperscript{15} Statements that impact a plaintiff’s business, trade, profession, or office may also be slander per se.\textsuperscript{16} A plaintiff may recover in such cases without proof of special damages.\textsuperscript{17}

Early American defamation law derives, at least in part, from English law.\textsuperscript{18} The tort of defamation protects the individual’s reputation in a community.\textsuperscript{19} As a dignitary tort, defamation law not only compensates for harm to one’s reputation, but also seeks “to vindicate the honor of the person defamed and to enforce society’s civility norms.”\textsuperscript{20} In contrast, under early English common law, a good reputation was a defense to nearly every crime.\textsuperscript{21} During the Middle Ages in England, one could seek a remedy for reputational harm in both secular and religious courts.\textsuperscript{22}

\begin{itemize}
  \item \textsuperscript{12} \textit{id.} \textsection{568(2)}. “The area of dissemination, the deliberate and premeditated character of its publication and the persistence of the defamation are factors to be considered in determining whether a publication is a libel rather than a slander.” \textit{id.} \textsection{568(3)}.
  \item \textsuperscript{13} \textit{id.} \textsection{571}.
  \item \textsuperscript{14} \textit{id.} \textsection{572}.
  \item \textsuperscript{15} \textit{id.} \textsection{574}.
  \item \textsuperscript{16} \textit{id.} \textsection{573}.
  \item \textsuperscript{17} \textit{id.} \textsection{570}.
  \item \textsuperscript{19} Veecher, \textit{supra} note 18, at 547 (observing that “the law of defamation professes to protect personal character and public institutions from destructive attacks, without sacrificing freedom of thought and benefit of public discussion”).
  \item \textsuperscript{20} David A. Anderson, \textit{Rethinking Defamation}, 48 ARIZ. L. REV. 1047, 1047, 1049 (2006) (noting that defamation is a dignitary tort and that attempts to “reduce it to a remedy for economic loss would be historically unfaithful, doctrinally radical, and destructive of important cultural values”).
  \item \textsuperscript{21} Veecher, \textit{supra} note 18, at 549 (citing 2 \textsc{Sir Frederick Pollack} & \textsc{Frederic William Maitland}, \textit{The History of English Law Before the Time of Edward I}, at 535–36 (1898)).
  \item \textsuperscript{22} Veecher, \textit{supra} note 18, at 546-47. “The Church, then, being answerable for the cleanliness of men’s lives, stayed the tongue of the defamer at one \textit{pro custodia morum} of the community, and \textit{pro salute animae} of the delinquent. The usual ecclesiastical penance for the offence was an acknowledgment of the baselessness of the imputation, in the
During the thirteenth and fourteenth centuries, seigniorial or manorial courts commonly heard defamation actions and punished defamation as sin.23 The late sixteenth century saw the decline of manorial courts, and the king’s courts more commonly began to hear defamation claims.24 Initially, defamation claims were heard only as special actions on the case.25 "The original common law doctrine of defamation, based upon the nature of the imputation, became stereotyped as the law of spoken defamation, or slander . . . ."26 Defamation claims heard “through the Star Chamber became the law of written and printed defamation, or libel.”27 After the abolition of the Star Chamber in 1641, libel became cognizable as a tort.28

Historically, strict liability applied to defamation claims on proof of a defamatory statement about a person that was communicated to a third person.29 The law presumed harm to one’s reputation from defamatory statements, thereby allowing the recovery of presumed and punitive

vestry room in the presence of the clergyman and church wardens of the parish, and an apology to the person defamed.” Id. at 551. Apart from the seigniorial and religious courts, the law provided a separate avenue of relief for defamation of certain members of the aristocracy by a statute “known as De Scandalis Magnatum.” Id. at 553 (citing Slanderous Reports Act, 1275, 3 Edw. 1, c. 34). The “limited aristocracy” protected by the Act included “Prelates, Dukes, Earls, Barons, and great men of the realm, and also of the Chancellor, Treasurer, Clerk of the Privy Seal, Steward of the King’s House, Justices of the one bench or the other, and of other great officers of this realm.” Id. at 553 n.3.

23. Veeder, supra note 18, at 549–50 (“More than a thousand years ago King Alfred provided that the slanderer should have his tongue cut out, unless he could redeem it with the price of his head.”).

24. Id. at 551–52, 557 (noting that the first defamation statute was enacted in the thirteenth year of Edward I, but had little effect until the ninth year of Edward II, when an additional defamation statute was enacted that permitted “corporal pence” as money payment in defamation cases).

25. Id.

26. Id. at 547 (citing Frank Carr, The English Law Of Defamation: With Especial Reference To The Distinction Between Libel And Slander, 18 L.Q.REV. 255 (1902)).

27. Id. at 546–47. In the case of King v. Lake in the Exchequer in 1670, Lord Chief Baron Hale first set forth the civil doctrine of libel. (1670) 145 Eng. Rep. 552.

28. David A. Anderson, supra note 20, at 1049 n.12 (citing RESTATEMENT OF TORTS § 568 cmt. b (1938)).

29. See, e.g., RESTATEMENT (SECOND) OF TORTS § 580 cmt. b (1977), observing that:

[T]he common law was to the effect that if the defendant was at fault in publishing the statement to a third party and it was reasonably understood to defame the other he was subject to liability . . . . This amounted to the imposition of strict liability or ‘liability without fault’ with regard to the falsity and the defamatory character of the statement.
Subsequently, however, the tort of slander required proof of special damages, unless the defamatory statement fell within one of the four slander per se categories.\textsuperscript{31}

Because "[e]very repetition of the defamation is a publication in itself, whether or not the person repeating the defamation attributes it to its source," anyone who repeats a defamatory statement is as liable as the original publisher.\textsuperscript{32} Traditional common law defamation rules distinguish, however, between the liability imposed on primary publishers and that imposed on distributors (also known as secondary publishers).\textsuperscript{33}

Primary publishers face strict liability for defamation.\textsuperscript{34} They "can be held liable for defamatory statements contained in their works even absent proof that they had specific knowledge of the statement's inclusion."\textsuperscript{35} In contrast, distributors or secondary publishers bear no liability for defamatory statements contained within materials they distribute absent "proof that they knew or had reason to know of the existence of damages.\textsuperscript{30}"

\textsuperscript{30} Restatement (Second) of Torts § 620 cmts. a–c (discussing presumed and punitive damages in Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974)); see also Carr, supra note 26, at 399 (reviewing the convoluted history of defamation and predicting that "the law will probably remain as it is to the end, for as Sir Frederick Pollock says, 'the law went wrong from the first in making the damage and not the insult the cause of action'"). But see Leslie Yalof Garfield, The Death of Slander, 35 Colum. J.L. & Arts 17, 52 (2011) (concluding that the distinction between libel and slander should be abrogated in favor of "one all encompassing tort of defamation").

\textsuperscript{31} See generally Restatement (Second) of Torts § 570–574; see also Freiwald, supra note 1, at 584 (noting that damages include compensation for actual injuries, "out of pocket losses, injury to reputation and community standing, personal humiliation, and mental anguish and suffering"); Terwilliger v. Wands, 17 N.Y. 54, 57, 60 (1858) (stating that "special damages must have been the natural, immediate and legal consequence of the words," and providing examples such as "the loss of a marriage, loss of hospitable gratuitous entertainment, preventing a servant or bailiff from getting a place, the loss of customers by a tradesman; and says that in general whenever a person is prevented by the slander from receiving that which would otherwise be conferred upon him, though gratuitously, it is sufficient").

\textsuperscript{32} Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1101 (9th Cir. 2009) (quoting Prosser and Keeton on Torts, supra note 2, § 113, at 799).

\textsuperscript{33} Id.; see also Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 139 (S.D.N.Y. 1991). Liability for defamation also has been separated into three categories of participants: "primary publishers, secondary publishers or disseminators, and those who are suppliers of equipment and facilities and are not publishers at all." Barnes, 570 F.3d at 1104 (citing Prosser and Keeton on Torts, supra note 2, § 113, at 803).

\textsuperscript{34} Dobbs, supra note 8, § 522.

\textsuperscript{35} Zerin v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) (citing Prosser and Keeton on Torts, supra note 2, § 113, at 810); see also Barnes, 570 F.3d at 1104 (citing Prosser and Keeton on Torts, supra note 2, § 113, at 810–11).
defamatory matter contained in [the materials] published.” An underlying policy reason for the distinction between imposing liability on primary publishers and secondary publishers or distributors is the degree of editorial control over the defamatory content. The greater that degree, “the higher the duty of care and corresponding liability.” Traditionally, primary publishers include “those entities that print or broadcast content.” For example, “[p]rimary publishers include most media outlets, such as the newspaper or book publisher that prints the statement, or the radio or television station that broadcasts it.” Distributors, or secondary publishers, include telegraph and telephone companies, libraries, newsstands, and book vendors. Distributors and secondary publishers generally are considered mere transmitters or conduits, rather than true publishers. While distributors and secondary publishers are generally liable for defamation, some authorities find no liability for the mere transmittal of defamatory statements delivered “by the post office, or . . . a phone or telegraph company” because the communication itself is not deemed to be a publication.

“Publication” in defamation law is a term of art. It refers to communicating the defamatory statement to someone “other than the person defamed.” Liability for publishing defamatory material may be imposed even if the individual is not the original publisher of the material. According to the Restatement (Second) of Torts, “[o]ne who intentionally and unreasonably fails to remove defamatory matter that he knows to be exhibited on land or chattels in his possession or under his

36. Zeran, 129 F.3d at 331 (quoting PROSSER AND KEETON ON TORTS, supra note 2, § 113, at 811) (internal quotation marks omitted).
38. Id.
39. Id.
40. RODNEY SMOLLA, 1 LAW OF DEFAMATION § 4:92 (2d ed.) (notes omitted).
41. PROSSER AND KEETON ON TORTS, supra note 2, § 113, at 810–11; DOBBS, supra note 8, § 522 (“[M]any others such as telegraph and telephone companies, libraries and news vendors are called transmitters, distributors or secondary publishers rather than primary publishers.”). “The disseminator is essentially a conduit, not an originator or promotor of content.” Id. “As to these, it seems clear that liability cannot be imposed unless the distributor knows or should know of the defamatory content in materials he distributes.” Id.
42. DOBBS, supra note 8, § 113, at 799.
43. SMOLLA, supra note 40, § 4:92 (notes omitted).
44. RESTATEMENT (SECOND) OF TORTS § 577(1) and cmt. b (1977).
45. Id. § 577(2).
control is subject to liability for its continued publication. Under this principle, even without knowledge or intent, ISPs may be held liable for defamatory content created by third parties, as liability is based upon knowledge or reason to know and “intentionally and unreasonably” failing to remove the harmful content.

Thus, absent the shield of § 230 immunity, Internet intermediaries that know or should have known of defamatory content—who generally would be considered distributors and secondary publishers in a traditional context—could be held liable if they fail to remove the content. Generally, the primary functions of intermediaries include: “access and storage providers, marketplace exchanges, buy/sell fulfillment, demand collection systems, auction brokers, virtual marketplaces, as well as search-engines, advertising networks, web aggregators, news syndicators or social networking sites.” Intermediaries generally “facilitate transactions between third parties.” Internet intermediaries provide “access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.” There are numerous forms of Internet intermediaries. For example, whether wired or wireless, Internet access and service providers “[p]rovide access to households, businesses, . . . government” and Internet

46. Id.
47. Id.
49. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OEC), THE ECONOMIC AND SOCIAL ROLE OF INTERNET INTERMEDIARIES 15 (2010), available at http://oecd.org/ieconomy/44949023.pdf. “The OECD is a unique forum where the governments of . . . democracies work together to address the economic, social and environmental challenges of globalization[,]” as well as to promote understanding of and a response to “new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population.” Id. at 2. The 34 OECD member nations are as follows: Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom and the United States. Members and Partners, OECD, http://www.oecd.org/about/membersandpartners (last visited April 22, 2015). By agreement, the OECD sought to achieve their goals “through an appropriate balance of laws, policies, self-regulation, and consumer empowerment.” Id. at 4. The Commission of the European Communities participates in the OECD. Id. at 2.
50. The Economic and Social Role of Internet Intermediaries, supra note 49, at 15.
51. Id.
52. Id.
cafes utilizing “physical transport infrastructure.” Examples of Internet service providers include Verizon, Comcast, T-Mobile, NTT, Internet Initiative Japan, Vodafone, Orange, and other large telecommunications companies. Some Internet service providers may also provide “web hosting, web page design, and consulting services related to networking software and hardware.”

Another form of intermediary provides the “[w]eb hosting, data processing and content delivery” services offered by entities such as “Navisite, Akamai, OVH, Easyspace, Rackspace, Register.com, Go Daddy, [and] GMO Internet Inc.” Web hosting services and data processing services, more commonly known as ‘cloud computing’ platforms,” are yet another form of intermediary. Internet search engines and portals like “Google, Yahoo!, Baidu, Naver, [and] MSN” also provide intermediary services. E-commerce intermediaries such as eBay, Amazon, Priceline.com, and Ali Baba facilitate buying and selling online. When paying for items online, payment systems like Visa, Paypal, and Mastercard are intermediaries used to process Internet payments. Participative or interactive intermediary forms used for social networking and content creation includes Facebook, YouTube, Ohmy News, and LinkedIn. Additional interactive or participative platforms include blogs, wikis, instant messaging, mobile, websites allowing critiques of written works, group-based aggregation, photo-sharing

53. Id. at 9, 11.
54. Id. at 9.
55. Id. at 11.
56. Id. at 9.
57. Id. at 9, 11, 39.
58. Id. at 9.
59. Id.
60. Id.
61. Id. Additional social media sites include MySpace, Mixi, “Twitter, Bebo, Orkut, Cyworld, Inceem, and ASmallWorld.” Id. at 14.
62. Id. at 14 (listing additional blogs, such as BoingBoing, Engadget, Skyrock, LiveJournal and Windows Live Spaces).
63. Id. (listing wiki sites, such as Wikipedia, PBWiki, Google Docs, and Wiktorary).
64. Id. (listing Skype, Trillian, and Windows Live Messenger media).
65. Id. (listing mobile version of social media sites).
66. Id. (listing Amazon, FanFiction.Net, and SocialText).
67. Id. (listing “[s]ites where users contribute links and rate them such as Digg, reddit,” as well as “[s]ites where users post tagged bookmarks such as del.icio.us”).
websites,\textsuperscript{68} podcasting,\textsuperscript{69} virtual worlds,\textsuperscript{70} online computer games,\textsuperscript{71} and video content and file-sharing sites.\textsuperscript{72}

In the United States, the defenses of truth and consent, as well as several privileges, are available to defendants in a defamation case.\textsuperscript{73} Traditionally, truth is an absolute defense and only requires proof that the statement was substantially true.\textsuperscript{74} Privileges available to defendants in defamation actions include absolute and qualified privileges.\textsuperscript{75} Absolute privileges completely immunize the defendant from liability for defamation.\textsuperscript{76} These absolute privileges apply, for example, to statements made during judicial\textsuperscript{77} and legislative\textsuperscript{78} proceedings and to statements made by federal government officials.\textsuperscript{79} Similarly, qualified privileges relieve a defendant of liability for defamation to protect the defendant's interest,\textsuperscript{80} the public's interest,\textsuperscript{81} and the interests of others.\textsuperscript{82}

Generally, there are four categories of qualified privileges.\textsuperscript{83} The first category is "the public interest privilege, to publish materials to public officials on matters within their public responsibility."\textsuperscript{84} The second

\begin{itemize}
\item \textsuperscript{68} Id. (listing Flickr and Kodak Gallery).
\item \textsuperscript{69} Id. (listing additional podcasts as iTunes, @Podder, FeedBurner (Google), and WinAmp).
\item \textsuperscript{70} Id. (listing DotSoul Cyberpark, Entropia Universe, Second Life, and Acive Worlds as examples of virtual worlds).
\item \textsuperscript{71} Id. (listing World of Warcraft, Club Pogo, Sims Online, Tomb Raider, and Lineage Ultima Online).
\item \textsuperscript{72} Id. (listing Daily Motion, YouTube, GyaO, and Crackle).
\item \textsuperscript{73} RESTATEMENT (SECOND) OF TORTS §§ 581A, 583, 585–592, 593–598 (1977).
\item \textsuperscript{74} Id. § 581A and § 581A, cmt. f. (Defendant "need not prove the literal truth of the allegedly defamatory accusation, 'so long as the imputation is substantially true so as to justify the "gist" or "sting" of the remark.'"); Maheu v. Hughes Tool Co., 569 F.2d 459, 465–66 (9th Cir. 1977).
\item \textsuperscript{75} Id. §§ 585–592, 593–598.
\item \textsuperscript{76} DOBBS, supra note 8, §§ 538–539.
\item \textsuperscript{77} RESTATEMENT (SECOND) OF TORTS §§ 585–589 (absolute privilege applies to judges, lawyers, jurors, and witnesses).
\item \textsuperscript{78} Id. §§ 590–590A (absolute privilege applies to legislators and witnesses testifying before legislature).
\item \textsuperscript{79} Id. § 585; see also id. at ch. 25, tit. B, intro. note.
\item \textsuperscript{80} Id. § 594.
\item \textsuperscript{81} Id. § 598.
\item \textsuperscript{82} Id. § 595.
\item \textsuperscript{83} DOBBS, supra note 8, § 544.
\item \textsuperscript{84} DOBBS, supra note 8, § 554; see also DAVID ELDER, DEFAMATION: A LAWYERS GUIDE § 2.26 (2014) (providing examples of public interest privilege, including "a victim's complaint of police misconduct to higher authority, a letter from a
category is “the privilege to publish to someone who shares a common interest, or relatedly, to publish in defense of oneself or in the interest of others.”

The third category of qualified privilege is fair comment, which “protect[s] the defendant’s statement of opinion about matters of public interest, provided the defendant truly stated the facts upon which the opinion was based.”

The final qualified privilege category is “the privilege to make a fair and accurate report of public proceedings and public documents.” Generally, these qualified privileges are conditional, such that a defendant may forfeit them by exceeding the scope of the privilege, engaging in excessive publication, or publishing with an improper purpose.

In 1964, the U.S. Supreme Court began to frame the traditional rules of defamation within a constitutional context. In New York Times v. Sullivan, the Court held that freedom of the press and freedom of speech required that public officials could not recover presumed and punitive damages for defamatory statements related to their official conduct absent proof of “actual malice.” A statement is made with actual malice if the speaker makes a statement “with knowledge that it was false or with reckless disregard of whether it was false or not.”

---

85. DOBBS, supra note 8, § 554; see also ELDER supra, note 84, § 2:24 (noting that the common interest privilege “is not limited to those with ‘identical, congruent, or even parallel’ interests” and includes “discussing examples of the common interest privilege including ‘inquiries made by plaintiff’s employer to construction management firm’s officers concerning plaintiff’s continuing effectiveness as construction coordinator, recommendations by an independent consultant hired by plaintiff’s employer to review its operations and make recommendations, [or] communications between an employer and outside review entity as to expenditures qualifying for insurance coverage’” (citations omitted)); id. § 2:25 (commenting that the privilege to publish in one’s defense or the defense of others generally concerns “one to whom the publisher is legally obligated to publish the information or is one to whom the publication is otherwise defensible,” such as “where defendant-doctor communicated with the patient’s lawyer regarding contemplated litigation, or where a doctor conferred with a charitable foundation regarding a patient he had referred for further treatment, or where an attorney communicated with the police or court administrator or a prospective vendor or to prospective defendants in a lawsuit on behalf of his client” (citations omitted)).

86. DOBBS, supra note 8, § 567.

87. Id. § 548 (stating that “fair and accurate reports of judicial, legislative, and official executive proceedings or reports arrests, and official hearings or meetings of public bodies” are privileged (citations omitted)).


90. Id. at 283–84.

91. Id. at 279–80.
A decade later, in *Gertz v. Robert Welch, Inc.*, the Court held that “so long as they do not impose liability without fault, the States may define for themselves the appropriate standard of liability for a publisher or broadcaster of defamatory falsehood injurious to a private individual.”92 When the plaintiff seeks presumed and punitive damages, the “actual malice” standard also applies to cases involving private individuals in matters of public concern.93 Subsequently, in *Philadelphia Newspapers v. Hepps*, a defamation case involving a private figure and a matter of public concern, the Court held that the plaintiff must prove the defamatory statement was false.94

On the other hand, the U.S. Supreme Court has ruled that defamatory statements about a private person in a matter of private concern require a less stringent standard of proof.95 In *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, the Court concluded that First Amendment concerns are reduced in such private defamation cases.96 Consequently, the Court held that in these cases “the state interest adequately supports awards of presumed and punitive damages—even absent a showing of ‘actual malice.’”97

Frequently, defamation in cyberspace is posted anonymously or pseudonymously.98 Online anonymity and pseudonymity present challenges for an individual seeking to recover for defamation because often it is difficult, if not impossible, to identify the creator of the defamatory content.99 The U.S. Supreme Court, however, does recognize

---

93. *Id.* at 325.
96. *Id.* at 759–61.
97. *Id.* at 761–63.
98. Doe v. Cahill, 884 A.2d 451, 456 (Del. 2005) (citing Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 895 (2000)); see also Bryant Storm, Comment, *The Man Behind the Mask: Defamed Without a Remedy*, 33 N. ILL. U. L. REV. 393, 402 (2013) (identifying challenges to filing suit against anonymous defamers including “(1) the court may find that the plaintiff does not satisfy the procedural requirements necessary to compel discovery, (2) the internet publisher may file a motion to quash the subpoena, or (3) the identifying information may no longer exist”).
99. See, e.g., Robert Danay, *The Medium Is Not the Message: Reconciling Reputation and Free Expression in Cases of Internet Defamation*, 56 McGill L.J. 1, 12–13 (2010) (observing that “since such communications are often impersonal and anonymous, . . . considered that there exists a greater risk that . . . defamatory remarks [will be] believed[,]” and “that defamation over the Internet had a greater potential to damage reputation as compared with ‘its less pervasive cousins’”).
a First Amendment right to anonymous speech.\textsuperscript{100} In \textit{McIntyre v. Ohio}, the Court stated that “the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry.”\textsuperscript{101} “[O]ne’s] decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.”\textsuperscript{102}

\textbf{B. MAKING OF THE CDA & LEGISLATIVE HISTORY}

Section 230 of the CDA responded to two recently decided cases:\textsuperscript{103} \textit{Stratton Oakmont, Inc. v. Prodigy Services Co.},\textsuperscript{104} and \textit{Cubby v.}


\textsuperscript{101} \textit{McIntyre}, 514 U.S. at 342.

\textsuperscript{102} \textit{Id}; discussing its decision in \textit{Talley v. California}, 362 U.S. 60 (1960), the \textit{McIntyre} court stated:

In \textit{Talley}, the Court held that the First Amendment protects the distribution of unsigned handbills urging readers to boycott certain Los Angeles merchants allegedly engaging in discriminatory employment practices. Writing for the Court, Justice Black noted that “[p]ersecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.” Justice Black recalled England’s abusive press licensing laws and seditious libel prosecutions, and he reminded us that even the arguments favoring the ratification of the Constitution advanced in the Federalist Papers were published under fictitious names. On occasion, quite apart from any threat of persecution, an advocate may believe his ideas will be more persuasive if his readers are unaware of her identity. Anonymity thereby provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent.


\textsuperscript{103} \textit{See, e.g.}, \textit{Barnes v. Yahoo! Inc.}, 570 F.3d 1096, 1101 (9th Cir. 2009) (noting that some of the “sister circuits have recognized, Congress enacted the Amendment in part to respond to a New York state court decision”) (citing \textit{Fair Hous. Council of San Fernando Valley v. Roommates.com}, 521 F.3d 1157, 1163 (9th Cir. 2008)); \textit{Zeran v. Am. Online, Inc.}, 129 F.3d 327, 331 (4th Cir. 1997); see also \textit{FTC v. Accusearch Inc.}, 570 F.3d 1187, 1195 (10th Cir. 2009). \textit{In Shtiamili v. Real Estate Group of New York, Inc.}, 17 N.Y.3d 281, 284 (2011), the Court of Appeals of New York, in a case of first impression, determined that the CDA barred “plaintiff’s claim against a Website operator arising out of allegedly defamatory comments posted to the Website.”
Although the legislative history of § 230 does not reference Cubby by name, Cubby is discussed and distinguished factually in Stratton, which is mentioned by name in the congressional records.

Cubby involved a defamation claim based on allegedly libelous statements that appeared on an online forum run by CompuServe. CompuServe was a pre-Internet ISP that provided subscribers with access to an electronic library and approximately 150 special interest forums. Subscribers could access the various forums using “electronic bulletin boards, interactive online conferences, and topical databases.” Rather than maintaining control over content posted on their various forums, CompuServe contracted with a separate, independent entity to “manage, review, create, delete, edit and otherwise control the contents of the Journalism Forum ‘in accordance with editorial and technical standards and conventions of style as established by CompuServe.’”

Developers of a competitor database filed suit against CompuServe based on statements posted on CompuServe’s Journalism Forum. The complaint alleged libel, business disparagement, and unfair competition. CompuServe moved for summary judgment, asserting “that it acted as a distributor, and not a publisher, of the statements, and [could not] be held liable for the statements because it did not know and had no reason to

104. Stratton Oakmont v. Prodigy, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995); see also 141 CONG. REC. 16025 (1995) (statement of Sen. Coats, “I want to be sure that the intent of the amendment is not to hold a company who tries to prevent obscene or indecent material under this section from being held liable as a publisher for defamatory statements for which they would not otherwise have been liable... Am I further correct that the subsection (f)(4) defense is intended to protect companies from being put in such a catch-22 position? If they try to comply with this section by preventing or removing objectionable material, we don’t intend that a court could hold that this is assertion of editorial content control, such that the company must be treated under the high standard of a publisher for the purposes of offenses such as libel.”); 141 CONG. REC. H8470 (daily ed. Aug. 4, 1995) (statement of Representative Cox, referring to Stratton decision as “backward”); 141 CONG. REC. H8471 (daily ed. Aug. 4, 1995) (statement of Rep. Goodlatte, criticizing Stratton decision).
108. Id.
109. Id.
110. Id.
111. Id. at 138. The alleged defamatory “statements included a suggestion that individuals at Skuttlebut gained access to information first published by Rumorville ‘through some back door’; a statement that Blanchard was ‘bounced’ from his previous employer, WABC; and a description of Skuttlebut as a ‘new start-up scam.’” Id.
112. Id.
know of [them].”113 The court reviewed the relevant law on liability of distributors and publishers for libel, as well as CompuServe’s control over the content posted on the Journalism Forum.114 The court determined that CompuServe offered essentially “an electronic, for-profit library” and thus was equivalent to a more traditional news vendor.115 The court held that the “inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information.”116 The court concluded that CompuServe maintained no more editorial control over the publications it provided than traditional purveyors of information did.117 Thus, “it would be no more feasible for CompuServe to examine every publication it carried for potentially defamatory statements than it would be for any other distributor to do so.”118

Having characterized CompuServe as a distributor for the sake of First Amendment concerns, the court determined that CompuServe’s liability for defamation should be determined based on whether it knew or had reason to know of the libelous content on its forum.119 As the plaintiff failed to demonstrate that CompuServe could have had such knowledge, the court granted CompuServe’s motion for summary judgment on the libel claim.120

The court in Stratton Oakmont v. Prodigy reached the opposite conclusion.121 It determined that the ISP was a publisher, thereby holding it liable for defamatory content posted on its Internet site by a third party.122 The ISP, Prodigy Services Company (Prodigy), maintained a

113. Id. at 143.
114. Id. at 140 (quoting Cianci v. New Times Publ’g Co., 639 F.2d 54, 61 (2d Cir. 1980)) (“one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it”); see also RESTATEMENT (SECOND) OF TORTS § 578 (1977). Regarding “news vendors, book stores, and libraries, however, New York courts have long held that vendors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation.” Cabby, 776 F. Supp. at 139 (quoting Lerman v. Chuckleberry Publ’g, Inc., 521 F. Supp. 228, 235 (S.D.N.Y. 1981)).
115. Cabby, 776 F. Supp. at 139.
116. Id. at 140.
117. Id.
118. Id.
119. Id. at 140-41.
120. Id. at 141.
122. Id.
computer network service with approximately two million subscribers. Prodigy hosted bulletin boards with information on various topics. These included the Money Talk forum, “allegedly the leading and most widely read financial computer bulletin board in the United States, where members [could] post statements regarding stocks, investments and other financial matters.”

Prodigy contracted with individuals to serve as leaders of its bulletin board discussions, as well as to encourage and increase usage of its services. Prodigy’s promotional materials marketed the company as an online community that seeks a “value system that reflects the culture of the millions of American families.” In support of its family-friendly objective, Prodigy developed and implemented policies, guidelines, and a software-screening program. Prodigy also made available to its bulletin board discussion leaders an emergency delete function to remove offensive materials posted by subscribers. When using the emergency delete function to remove offensive messages, the board leaders could select from a range of pre-prepared messages to the poster. These variously characterized posts as “solicitation, bad advice, insulting, wrong topic, off topic, bad taste, etcetera.”

On two occasions in October 1994, an unidentified user posted allegedly defamatory messages on Money Talk concerning Stratton Oakmont, Inc. (Stratton), a securities investment banking firm, and its president. The defamatory statements alleged, among other things, that one of Stratton’s initial public offerings constituted a “major criminal fraud,” that Stratton “was a cult of brokers who either lie for a living or get fired,” and that Stratton’s president had committed criminal and fraudulent acts related to an initial public offering. Based on these

123. Id.
124. Id.
125. Id.
126. Id.
127. Id. at *2.
128. Id.
129. Id.
130. Id.
131. Id. at *2–3.
132. Id. at *1.
133. Id. at *1. Jordan Belfort, who was indicted on securities fraud and money laundering charges in 1998, is one of the founders of the Stratton Oakmont brokerage firm. ‘Wolf of Wall Street’ Distributors Seek Dismissal of Use-of-Likeness Suit, WESTLAW J. ENT. INDUSTRY, May 7, 2014, at 1. The Wolf of Wall Street is an Oscar nominated movie that is based on Mr. Belfort’s memoir of the same name. See THE WOLF OF WALL
statements, Stratton filed a ten-count suit against Prodigy, which included a libel per se claim seeking $200 million in damages.\textsuperscript{134}

Prodigy sought partial summary judgment, focusing on the issues of (1) whether Prodigy is considered a publisher or distributor, and (2) whether the Money Talk bulletin board leader “acted with actual and apparent authority as Prodigy’s ‘agent’ for the purposes of the claims in this action.”\textsuperscript{135} Regarding Prodigy’s status as a publisher or distributor, the court examined whether Prodigy “exercised sufficient editorial control over its computer bulletin boards to render it a publisher.”\textsuperscript{136} Prodigy argued that it was not a publisher but rather a distributor in conformance with the prior decision in Cubby.\textsuperscript{137}

The court found, notwithstanding the decision in Cubby, that Prodigy was a publisher, based, in part, on documentary evidence of Prodigy’s policies and content guidelines.\textsuperscript{138} The court distinguished the activities of the ISP in Cubby.\textsuperscript{139} Unlike the Cubby ISP, Prodigy had publically represented that it controlled the content on its computer bulletin boards and had touted “its automatic software screening program, and the Guidelines which Board Leaders [were] required to enforce.”\textsuperscript{140} The court further determined that Prodigy’s acceptance of the benefits of editorial control subjected it to a higher standard of liability.\textsuperscript{141} In contrast, it noted that the ISP in Cubby and other ISPs had made “no such choice.”\textsuperscript{142} Consequently, the court held that the bulletin board leaders had acted as Prodigy’s agent.\textsuperscript{143} Thus, Prodigy’s efforts to develop and implement policies and guidelines to limit or restrict access to objectionable material posted on its online sites resulted in the court’s determination that Prodigy was liable as a publisher for defamatory statements posted on its forum by an unidentified user.\textsuperscript{144}

\textsuperscript{134} \textit{Stratton}, 1995 WL 323710, at *1.
\textsuperscript{135} Id.
\textsuperscript{136} Id. at *3.
\textsuperscript{137} Id. at *4–5.
\textsuperscript{138} Id. at *3.
\textsuperscript{139} Id.
\textsuperscript{140} Id. at *4.
\textsuperscript{141} Id.
\textsuperscript{142} Id. at *5.
\textsuperscript{143} Id. at *6.
\textsuperscript{144} Id. at *3–6.
III. SECTION 230
A. CONTENTS OF § 230

As titled, § 230 offers “[p]rotection for private blocking and screening of offensive material” on the Internet.145 When ISPs voluntarily implement a process to screen and block access to “offensive materials,” the “[g]ood[s]amaritan” provision in subsection (c) protects ISPs from liability.146 Importantly, subsection (c)(1) addresses the status of ISPs and expressly states “[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.”147 Subsection (c)(2) protects ISPs from civil liability when ISPs “restrict access to or availability of material” that the ISPs deem to be “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.”148 This statutory protection against civil liability applies even if the restricted materials are “constitutionally protected.”149 However, subsection (f)(3) specifically denies immunity to ISPs that have created the objectionable material themselves.150

Subsection (d) mandates that ISPs provide their customers with a notice of content blocking equipment at the time of entering an agreement.151 Specifically, the ISP shall provide the customer with notice of the commercial availability of “parental control protections (such as computer hardware, software, or filtering services) . . . that may assist the customer in limiting access to material that is harmful to minors.”152 The mandatory notice must provide customers with current providers of parental control protections.153 The statute protects ISPs from civil liability when they provide “information content providers or others the technical means to restrict access to material” the ISPs deem to be “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise

146. § 230(c).
147. § 230(c)(1).
148. § 230(c)(2)(A).
149. Id.
150. § 230(f)(3); see also § 230(c)(1).
151. § 230(d).
152. § 230(d). Section 230(f)(4) defines “access software provider” as “a provider of software (including client or server software), or enabling tools that do any one or more of the following: (A) filter, screen, allow, or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.”
153. § 230(d).
objectionable.\footnote{154} In this way, the statute removes the prospect of the ISPs incurring civil liability in the course of restricting or limiting access to content the ISPs consider offensive.\footnote{155} By so doing, the CDA recognizes the importance of maintaining the Internet as a free market for ease of access to informational, educational, and entertainment resources, while bowing to concerns about potentially objectionable content.\footnote{156}

Section 230 specifically notes that it does not preempt certain federal and state laws.\footnote{157} Regarding federal law, it states that the statute has no effect on communications privacy law,\footnote{158} intellectual property law,\footnote{159} and criminal law.\footnote{160} In regard to state laws, § 230 provides that “[n]othing in this section shall be construed to prevent any State from enacting any State law that is consistent with this section.”\footnote{161} Thus, state laws are not preempted so long as they do not conflict with § 230. However, § 230 also states 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.”\footnote{162}

\footnotesize

154. §§ 230(c)(2)(A)-(B). The statute defines “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.” § 230(f)(3).

155. See § 230(c)(2)(A).

156. See § 230(c)(2).

157. § 230(e).

158. § 230(e)(4) (“Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar state law.”).

159. § 230(e)(2) (“Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.”); § 230(e)(3) (“Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section.”); § 230(e)(4) (“Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 . . . or any similar State law.”); see also CYBERsitter, LLC v. Google Inc., 905 F. Supp. 2d 1080 (C.D. Cal. 2012) (trademark infringement not barred by CDA); Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1322–324 (11th Cir. 2006) (resolving a CDA question on other grounds); Ohio State Univ. v. Skreened Ltd., 16 F. Supp. 3d 905, 918 (S.D. Ohio 2014) (noting that the § 230 “immunity provision does not apply in the trademark context of a state law right of publicity claim”); Ford Motor Co. v. GreatDomains.com, Inc., No. 00-CV-71544-DT, 2001 WL 1176319, at *1 (E.D. Mich. Sept. 25, 2001) (noting that § 230(e)(2) “unambiguously precludes . . . immunity” in the context of federal trademark laws).

160. § 230(e)(1) (“Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute.”).

161. § 230(e)(3).

162. See id.
B. LEGISLATIVE HISTORY OF THE CDA

In 1996, Congress engaged in a comprehensive revision of the Telecommunications Act. In the revision, Congress sought to “reduce regulation and encourage ‘the rapid deployment of new telecommunications technologies.’” The major components of the statute aimed “to promote competition in the local telephone service market, the multichannel video market, and the market for over-the-air broadcasting.”

Congress incorporated the CDA of 1996 in its revisions of the Telecommunications Act. Unquestionably, Congress intended § 230 to overrule Stratton. Indeed, the House Conference Report on the Cox-Wyden version of the bill proposing the enactment of § 230 by the House of Representatives expressly stated that “[t]he conferees believe that such decisions create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.”


167. H.R. REP. NO. 104-458, at 191, 194 (Conf. Rep.) (1996); 141 Cong. Rec. 22044–46 (Cox-Wyden Proposal offered by Chris Cox (R-CA) and Ron Wyden (D-OR)); see also Robert Cannon, The Legislative History of Senator Exon’s Communications Decency Act: Regulating Barbarians on the Information Superhighway, 49 FED. COMM. L.J. 51, 63 (1996) (“In the Conference Report, the conferees specifically stated that they were overturning Stratton.”); Freiwald, supra note 1, at 596 (stating that § 230 was enacted to overrule Stratton Oakmont v. Prodigy and nothing more).


The Cox-Wyden Amendment, the foundation for what is now § 230 of the CDA, stated that it “sought to further First Amendment and e-commerce interests on the Internet while also promoting the protection of minors.” Thus, proponents of the CDA promoted it, in part, as a means to protect children from access to online pornography and other obscene materials. Senator Exon argued “the worst, most vile, most perverse pornography is only a few click-click-clicks away from any child on the Internet.” To further convince his Senate colleagues of the potentially harmful images lurking in cyberspace, Senator Exon had a staffer prepare as demonstrative evidence the now famous “blue binders” of images of online pornography. Thus, through the CDA, Congress attempted to restrict certain types of speech online, which necessarily implicated First Amendment free speech protections.

The CDA also sought to encourage the Internet industry to self-regulate its transmission of indecent and obscene content. Congress considered self-regulation a better alternative to government interference in an unfamiliar, rapidly-developing new medium. Decisions like Stratton, however, provided disincentives for self-regulation given the risk of exposure to liability. Section 230 expressly addressed that concern and

170. Barzel, 333 F.3d at 1028 (citing 141 CONG. REC. H8469-72 (referring to “[s]tatements of Representatives Cox, Wyden, Lofgren, and Goodlatte”)).
173. See id. at 15503-04. “At the request of Senator Exon, a friend downloaded from the Internet a collection of pornography. This was gathered in a blue folder and made accessible at Senator Exon’s desk on the Senate floor so that everyone could observe the ‘filth’ that was accessible to every boy and girl in this country.” Cannon, supra note 167, at 64.
174. See Reno v. ACLU, 521 U.S. 844, 857–58 (1997). The First Amendment of the U.S. Constitution provides as follows: “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.” U.S. CONST. AMEND. I.
175. Reno, 521 U.S. at 857–58.
177. Theoretically, self-regulation could be accomplished through market forces. These forces, driven in part by the need of consumers for confidence in the reliability of the information provided, would essentially create a parallel universe of ISPs: those that are responsible and reliable, and those that are not.
provides protection to ISPs that voluntarily act to restrict access to objectionable materials. 178

The CDA intended to protect ISPs from liability in two respects when the ISPs voluntarily implemented software programs to block, restrict, screen, or otherwise limit access to obscene content from their sites. First, it aimed to protect the ISPs from liability to the purveyors of such content. 179 Second, the “intent of the amendment [was] not to [allow] a company who tries to prevent obscene or indecent material under this section [to] be[] held liable as a publisher for defamatory statements for which they would not otherwise have been liable.” 180 Accordingly, in response to the court’s determination in Stratton that the ISP was a publisher, Congress determined that ISPs are neither publishers nor speakers, and provided immunity to ISPs for content provided by third parties when the ISPs implemented blocking policies or provided its users with information on how to accomplish the same. 181

C. JUDICIAL INTERPRETATION OF § 230

Although the U.S. Supreme Court has struck down portions of the CDA as unconstitutional, § 230 of the CDA, including its “Good Samaritan” immunity provision, survives. 182 A substantial majority of the United States Circuit Courts of Appeal have determined that § 230 immunizes ISPs from liability for online content provided by a third party. 183 These courts “have interpreted the CDA to establish broad

178. § 230(c)(2).
179. See id.
181. See, e.g., Freiwald, supra note 1, at 596.
‘federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.’

1. CDA Immunity from Defamation Upheld

The United States Court of Appeals for the Fourth Circuit was one of the first federal courts of appeal to address the issue of § 230 immunity for an ISP related to content posted on its Internet sites by third parties. In Zeran v. America Online, Inc., an unidentified individual posted advertisements on AOL offering for sale t-shirts, key chains, bumper stickers, and other items “featuring offensive and tasteless slogans related to the April 19, 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City.” The advertisements instructed prospective purchasers to call “Ken” and listed his home telephone number in Seattle, Washington. In fact, the advertisements were a cruel prank played by an anonymous poster on Kenneth Zeran.

As a result of the offensive online advertisements, Zeran received threatening and harassing telephone calls, including death threats. Zeran could not change his telephone number because he operated an at-home business that relied on his telephone communications with his customers. Zeran contacted AOL to explain the problem and requested that AOL remove the advertisement. An AOL representative assured Zeran the advertisement would be removed; however, the next day, an anonymous person posted a similarly offensive advertisement with additional items for sale, and again listed Zeran’s home telephone number as the contact. Zeran contacted local police and the Federal Bureau of Investigation (FBI) as the number of violent, threatening telephone calls escalated to a call every two minutes.


186. Id. at 329.
187. Id. at 329.
188. Id.
189. Id.
190. Id.
191. Id.
192. Id.
193. Id.
Zeran eventually filed a negligence claim in the United States District Court for the Western District of Oklahoma against America Online, Inc. (AOL), based on AOL’s failure “to remove the defamatory posting promptly, to notify its subscribers of the message’s false nature, and to effectively screen future defamatory material.”\textsuperscript{194} Subsequently, the case was transferred to the Eastern District of Virginia.\textsuperscript{195} Zeran alleged that AOL owed a duty to its subscribers “to notify [them] of the message’s false nature, and to effectively screen future defamatory material.”\textsuperscript{196} In response, AOL raised § 230 of the CDA as a defense to Zeran’s complaint and filed a motion for judgment on the pleadings.\textsuperscript{197} AOL argued its § 230 defense immunized ISPs from liability for online postings by a third party.\textsuperscript{198} The district court rejected Zeran’s claim that AOL owed a duty to remove the defamatory postings promptly after Zeran had notified AOL of the offensive postings and the resulting violent threats.\textsuperscript{199} The court granted AOL’s motion for judgment on the pleadings, and Zeran appealed.\textsuperscript{200}

The Court of Appeals for the Fourth Circuit considered the availability of § 230 as a defense to Zeran’s claims.\textsuperscript{201} In construing the statute, the court first determined that “[b]y its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.”\textsuperscript{202} The court also considered Congress’s purposes and policies in enacting the statute.\textsuperscript{203} These included protecting the growth of an

\textsuperscript{194} \emph{Id.} at 330. Prior to filing his complaint against AOL, Zeran also filed a separate suit against the owner of KRKO, an Oklahoma City radio station. \emph{Id.} at 329. A KRKO announcer received a copy of the offensive AOL posting and read it on air. \emph{Id.} Zeran subsequently “was inundated with death threats and other violent calls from Oklahoma City residents.” \emph{Id.} Zeran’s complaint against the owner of KRKO radio station sought damages for defamation, false light invasion of privacy, and intentional infliction of emotional distress. Zeran v. Diamond Broad. Inc., 19 F. Supp. 2d 1249, 1252–54 (W.D. Okla. 1997) (summary judgment granted in favor of radio station owner finding insufficient evidence of injury to reputation on the defamation claim, and denying claim that the radio station’s negligence resulted in false light invasion of privacy and intentional infliction of emotional distress), aff’d, 203 F.3d 714 (10th Cir. 2000).

\textsuperscript{195} \emph{Id.}, 129 F.3d at 329.

\textsuperscript{196} \emph{Id.} at 330.

\textsuperscript{197} \emph{Id.} at 328–30.

\textsuperscript{198} \emph{Id.}

\textsuperscript{199} \emph{Id.} at 330.

\textsuperscript{200} \emph{Id.}

\textsuperscript{201} \emph{Id.}

\textsuperscript{202} \emph{Id.}

\textsuperscript{203} \emph{Id.} at 330–33.
Internet that fosters free speech and incentivizing self-regulation in the Internet industry with minimal government interference.204 The court also observed that Congress had enacted § 230 to respond to Stratton Oakmont, Inc. v. Prodigy Services Co.205

Zeran had argued on appeal that § 230 immunizes publishers, but does not protect distributors from liability for online content posted by a third party.206 Zeran contended that AOL functioned as a distributor of such content.207 The court noted the distinction between distributors and publishers, but concluded that distributors also may be classified as publishers.208 The court determined that Zeran placed “too much importance to the presence of the distinct notice element in distributor liability.”209 The court stated that “[t]he simple fact of notice surely cannot transform one from an original publisher to a distributor in the eyes of the law.”210 However, the court ultimately rejected Zeran’s argument that § 230 immunity is not available to distributors.211 It found that when AOL receives notice of defamatory material, AOL’s position is no different than that of a traditional publisher.212 The court relied on Prosser’s hornbook in its discussion of whether distributors should be treated as original publishers for the proposition that those who are in the business of disseminating information intentionally are publishers, with or without notice of the information’s content.213 Despite Zeran’s claim to the contrary—that § 230 does not shield service providers that have notice of the defamatory content—the court held that “[s]ection 230 . . . plainly immunizes computer service providers like AOL from liability for information that originates with third parties.”214 Under the Zeran analysis, when a distributor receives notice of the defamatory material, it “must decide whether to publish, edit, or withdraw the posting.”215 Thus, in the court’s view, the distributor becomes a publisher and is entitled to § 230 immunity.216

204. Id.
205. Id. at 331.
206. Id. at 331–32.
207. Id.
208. Id. (quoting PROSSER AND KEETON ON TORTS, supra note 2, § 113).
209. Id. at 332.
210. Id.
211. Id. at 334–35.
212. Id.
213. Id. at 332.
214. Id. at 328.
215. Id. at 332.
216. Id. at 332–33.
A number of commentators have criticized the Zeran decision.\textsuperscript{217} Some argued that, “[b]y defining distributors as publishers, the Zeran court effectively eliminated all defamation liability for third-party content posted on the Internet.”\textsuperscript{218} One scholar argues that the interest in protecting one’s reputation is a dignitary interest protected by the Ninth Amendment that should not be diminished by “an expansive reading of the First Amendment.”\textsuperscript{219} Such a sweeping change in the law would require clear evidence of Congressional intent to preempt all state law defamation claims.\textsuperscript{220} However, § 230 and its legislative history are silent on the issue.\textsuperscript{221}

Other critics stress that § 230(c)(2)(A) grants immunity from civil liability only to ISPs that voluntarily engage, as Congress intended, in acts that “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, whether or not such material is constitutionally protected.”\textsuperscript{222} Thus, by its own terms, § 230 protection appears limited to ISPs that engage in some manifest action to restrict, block, or screen access to objectionable speech.\textsuperscript{223} These critics note that the gist of Zeran’s complaint was that AOL took no action at all to block the speech that plagued him.\textsuperscript{224} Consequently, § 230 immunity should not

\begin{itemize}
\item \textsuperscript{217} A string of article cites are provided in Barrett v. Rosenthal, 9 Cal. Rptr. 3d 142, 154 n.8 (Cal. Ct. App. 2004), reproduced infra note 345.
\item \textsuperscript{218} Oliva Medenica, The Immutable Tort of Cyber-Defamation, J. INTERNET L., Jan. 2008, at 3, 5 (observing that § 230 immunity has been applied not only in defamation cases but also in negligence, unfair competition, breaches of contract and state securities laws, and cyberstalking) (citing Doe v. Am. Online Inc., 783 So. 2d 1101, 1013–1117 (Fla. 2001), cert. denied, 534 U.S. 891 (2001) (negligence); Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077 (C.D. Cal. 2004) (unfair competition); Morrison v. Am. Online, Inc., 153 F. Supp. 2d 930, 934 (N.D. Ind. 2001) (defamation)).
\item \textsuperscript{219} Cristina Carmody Tilley, Rescuing Dignitary Torts from the Constitution, 78 BROOK. L. REV. 65, 121 (2012) (arguing that Ninth Amendment “dignitary rights are protected from the diminishment that necessarily follows from an expansive reading of the First Amendment”).
\item \textsuperscript{220} See, e.g., Theodor v. Superior Court, 501 P.2d 234, 237 (Cal. 1972) (stating that “it should not be presumed that the Legislature in the enactment of statutes intends to overthrow long-established principles of law unless such intention is made clearly to appear either by express declaration or by necessary implication” (internal quotation marks omitted)).
\item \textsuperscript{221} See, e.g., Medenica, supra note 218, at 5.
\item \textsuperscript{222} § 230(c)(2)(A); see also Barrett v. Rosenthal, 9 Cal. Rptr. 3d at 154 n.8 (providing a string of article cites, reproduced infra note 345).
\item \textsuperscript{223} See, e.g., Medenica, supra note 218, at 5.
\item \textsuperscript{224} See, e.g., Barrett, 9 Cal. Rptr. 3d at 154 n.8 (providing a string of article cites) (reproduced infra note 345).
\end{itemize}
have applied. By protecting AOL from liability, the Zeran court well exceeded the intended scope of § 230’s immunity provision.225

Yet another scholar argues that court decisions construing § 230 merely exacerbate Congress’ error in enacting the Act.226 For example, in Zeran, the district court “sanctioned the one-sided bargain that permitted intermediaries to learn of egregious defamation on their systems but take no action.”227 In finding the ISP immune from liability, the district court’s reasoning was unclear as to the significance of notice in the distinction between primary publishers and distributors.228 In affirming that § 230 confers immunity to the ISP, the Court of Appeals for the Fourth Circuit similarly misconstrued the importance of notice in its determination that “notice surely cannot transform one from an original publisher to a distributor in the eyes of the law.”229 Both the Fourth Circuit and the district court failed to consider the principle that notice “does not transform a distributor into a publisher, but rather subjects a distributor to liability appropriate to its knowledge if it fails to respond to complaints.”230 Further, the Fourth Circuit determined that “notice-based liability would discourage intermediary monitoring” and, potentially, could lead to self-censorship, thereby limiting, rather than, encouraging free speech.231

Another scholar argues that there is little support for the Zeran court’s determination that there is no distinction between publishers and distributors, which results in blanket immunity under § 230 for both types of publishers.232 Among other things, she recommends that the traditional

225. See Medenica, supra note 218, at 9. One commentator observed that the overly broad interpretation of § 230 is ineffective and “it treats internet publishers differently than print publishers merely because they are on the internet, and it protects and immunizes a less deserving kind of speech[,]” namely non-political “[s]peech that targets private persons.” Storm, supra note 98, at 421.
226. Freiwald, supra note 1, at 637–42.
227. Id. at 640.
228. See id.
229. Id. (quoting Zeran v. Am. Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997)).
230. Id. The author further noted that at least one court recognized its role in exacerbating the one-sided bias and stated, as it adopted the reasoning of Zeran, that through “some sort of tacit quid pro quo arrangement with the service provider community, Congress has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted.” Id. at 644 (quoting Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.D.C. 1998)).
231. Id. at 640–41.
232. Medenica, supra note 218, at 8 (“I find it hard to believe, however, that Congress meant this legislation to provide the all-encompassing immunity it has become.”).
distinction between distributors and publishers should be revived.\textsuperscript{233} In reviewing the legislative history, including the purposes and objectives of Congress, one of which was to overrule the \textit{Stratton Oakmont v. Prodigy} decision, the commentator concludes that the Zeran court broadened “the scope of the \textit{Stratton} holding well beyond the intended limits of § 230.”\textsuperscript{234} She further concludes that reviving distributor liability, which is based on knowledge or reason to know of the defamatory statement, is consistent with the Act’s purpose to encourage self-monitoring.\textsuperscript{235}

Other scholars agree with these criticisms of the Zeran decision.\textsuperscript{236} One scholar posits that Zeran’s overly broad interpretation of § 230 immunity has resulted in “the immunization of ‘parties surely not within the intended scope of Section 230.’”\textsuperscript{237} He further states that Zeran’s rigid construction of § 230 “does not allow for situations where immunity should not be extended despite third-party authorship” and, contrary to the Act’s purpose, eliminates any incentive to self-monitor.\textsuperscript{238} Still other Zeran critics similarly contend that the decision provides more extensive immunity from defamation liability than Congress intended, in light of both the legislative history and plain language of the statute.\textsuperscript{239}

\textsuperscript{233} \textit{Id.} at 8–9.
\textsuperscript{234} \textit{Id.} at 9.
\textsuperscript{235} \textit{Id.}
\textsuperscript{237} \textit{Id.} at 667 (quoting Gregory M. Dickinson, Note, An Interpretive Framework for Narrower Immunity Under Section 230 of the Communications Decency Act, HARV. J.L. & PUB. POL’Y 863, 873 (2010)).
\textsuperscript{238} \textit{Id.} (quoting Gregory M. Dickinson, Note, An Interpretive Framework for Narrower Immunity Under Section 230 of the Communications Decency Act, HARV. J.L. & PUB. POL’Y 863, 873 (2010)).
Subsequently, numerous federal courts of appeal have reached the same conclusion as the court in Zeran.240 In 2000, the Court of Appeals for the Tenth Circuit considered whether AOL, as an ISP, had forfeited § 230 immunity when it provided access to allegedly inaccurate information regarding a company’s publicly traded stock.241 A manufacturer and designer of corporate finance computer software, Ben Ezra, Weinstein, and Company (Ben Ezra), sought damages and injunctive relief against AOL on theories of defamation and negligence.242 Ben Ezra “alleged that on three separate occasions [AOL] published inaccurate information concerning [Ben Ezra’s] stock price and share volume.”243 Affirming the district court’s grant of summary judgment for AOL, the Court of Appeals noted that Ben Ezra had failed to present any evidence that AOL, “in whole or in part,” had created or developed the incorrect information.244 Citing with approval the Zeran decision, the court concurred with the Fourth Circuit’s determination that § 230 proscribe ISP liability for online information content created by third parties.245 More recently, the Tenth Circuit reaffirmed its position.246

240. See, e.g., Ben Ezra, Weinstein & Co. v. Am. Online, Inc., 206 F.3d 980, (10th Cir. 2000) (discussed infra); Green v. Am. Online Inc., 318 F.3d 465 (3rd Cir. 2003) (discussed infra); Johnson v. Arden, 614 F.3d 785 (8th Cir. 2010) (finding ISP immune under § 230; ISP was not an information content provider or developer, did not solicit defamatory statements, and thus was immune from liability for state tort claims for defamatory statements posted by third party); Universal Commc’n Sys., Inc. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007) (finding Internet message board operator immune from liability for defamatory statements posted by pseudonymous posters; user created information content); Carafano v. Metroplash, Inc., 339 F.3d 1119 (9th Cir. 2003) (finding Internet dating service immune from liability for defamation and other tort claims arising from anonymous posting creating fictitious profile with sexually suggestive statements, using the name, home address, and email address of actress; defendant and minor son forced to reside in hotels and other places because of safety concerns); Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003); Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997); Giordano v. Romeo, 76 So. 3d 1100, 1101–02 (Fla. Dist. Ct. App. 2011) (holding website operator absolutely immune). Numerous state courts also have followed the Zeran analysis on the CDA’s grant of immunity to ISPs. See infra note 266.

241. Ben Ezra, 206 F.3d at 983.

242. Id.

243. Id.

244. Id. at 983, 985–86. The court observed that despite repeated questions during oral arguments concerning evidence in the record in support of Ben Ezra’s claim that AOL developed or created the inaccurate information, counsel for Ben Ezra “could not identify any evidence.” Id. at 985 n.5.

245. Id. at 986, citing Zeran, 129 F.3d at 327, 330.

246. See, e.g., Getachew v. Google, Inc., 491 F. App’x 923 (10th Cir. 2012) (holding search engine immune from plaintiffs federal and state law claims).
In 2003, the Courts of Appeals for the Third and Ninth Circuits also followed the Zeran court’s holding. In *Green v. AOL*, a subscriber filed suit against AOL and two unidentified AOL subscribers alleging, among other things, defamation, negligence, and intentional infliction of emotional distress. The claim arose from AOL’s failure to police the activities of third parties who, on one occasion, had launched malicious software that temporarily disabled the plaintiff’s computer, and, on another occasion, had posted defamatory comments about the plaintiff in an AOL chat room. Quoting Zeran, the Third Circuit rejected the plaintiff’s claim, holding that § 230 “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.’” Also quoting Zeran, the Ninth Circuit barred a claim arising from the fraudulent and cruel posting of a profile in the plaintiff’s name on an online dating service.

The First, Sixth, Seventh, Eighth, and Eleventh Circuit Courts of Appeals have followed suit in rejecting claims against ISPs involving content posted by third parties. In *Universal Communications Systems, Inc. v. Lycos, Inc.*, the First Circuit opined that the broad immunity “effectuate[d] Congress’s ‘policy choice . . . not to deter harmful online speech through the . . . route of imposing tort liability on companies that serve as intermediaries for other parties’ potentially injurious messages.” The court disregarded the ISP’s notice of the
misinformation posted in this case, concentrating instead on the plaintiff's failure to demonstrate that the ISP had in any way created or facilitated the misinformation through "[the ISP]'s registration process or... link structure."²⁵⁹ The Seventh Circuit ruled in favor of the ISP Craigslist in an action asserting that a discriminatory online posting of a housing advertisement had violated the Fair Housing Act.²⁶⁰ Observing that Craigslist had neither directly nor indirectly fostered the discriminatory content, the court observed that one "cannot sue the messenger just because the message reveals a third party's plan to engage in unlawful discrimination."²⁶¹ More recently, the Court of Appeals for the Eleventh Circuit affirmed the district court's determination that Google was immune to the plaintiff's defamation claim despite the plaintiff's contention that the defendant "manipulated its search results to prominently feature the article at issue."²⁶² Finally, in dicta, the Sixth Circuit absolved the travel ISP Tripadvisor of any liability under the CDA for including the plaintiff's hotel on its dirtiest hotel of the year list,²⁶³ a list compiled from the results of comments posted in its survey of public users.²⁶⁴

Predictably, federal district courts have followed the lead of the majority of circuit courts of appeal.²⁶⁵ To date, the number of such cases exceeds thirty.²⁶⁶ The claims asserted range from defamation, invasion of

²⁵⁹ Id. at 420.
²⁶¹ Id.
²⁶² Dowbenko, 582 Fed. App'x at 805.
²⁶³ Seaton v. Tripadvisor LLC, 728 F.3d 592, 599 n.8 (6th Cir. 2013) ("We note that even if the complaint or proposed amended complaint had alleged that Trip Advisor's users' statements are defamatory, Tripadvisor cannot be held liable for its users' statements under the Communications Decency Act, 47 U.S.C. § 230(c)(1).").
²⁶⁴ Id. at 594.
privacy, and negligence, to unfair trade practices. Following the reasoning in Zeran, the district courts have held that ISPs are immune from liability for various state law claims. A number of state courts have also decided that § 230 immunity barred the claims alleged.
“Nevertheless, § 230(c)(1) ‘was not meant to create a lawless no-man’s-land on the Internet.’”

2. CDA Immunity Defense Does Not Apply

In 2008, the Ninth Circuit departed from the Zeran line of cases, holding that § 230 does not necessarily protect an ISP from liability for postings by third parties. *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC* concerned an Internet website service, Roommates.com ("Roommates"), which matched owners of spare rooms to people seeking accommodation. 270 To participate in the roommate matching service, subscribers created a profile by answering a series of questions. 271 Subscribers provided, among other information, their name, email address, location, and additional comments. 272 Roommates also required subscribers to state their sex, sexual orientation, and whether children would be living with them. 273 Roommates prepared a subscriber profile from this information that included the subscriber’s description, preferences, and a pseudonym. 274 The Fair Housing Councils of the San Fernando Valley and San Diego ("Councils") filed suit against Roommates in federal court, alleging, among other things, that Roommates’s service violated federal fair housing laws. 275 The federal district court held that § 230 immunized Roommates from liability. 276 Councils appealed. 277

On appeal, the Court of Appeals for the Ninth Circuit observed that Congress had enacted § 230 in response to *Stratton Oakmont, Inc. v. Prodigy Services Co.* 278 Reviewing the CDA’s history, the Court opined that Congress had sought to protect ISPs from liability for removing, blocking, screening, and restricting access to obscene and otherwise

---

269. *Hare,* 2012 WL 3773116, at *16 (quoting *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC,* 521 F.3d 1157, 1164 (9th Cir. 2008)).
270. *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC,* 521 F.3d 1157, 1161 (9th Cir. 2008)
271. Id.
272. Id.
273. Id.
274. Id. at 1161–62.
275. Id. at 1162, 1162 n.4 (quoting *Fair Housing Act,* 42 U.S.C. § 3604(c) (2012) and CA. GOV. CODE § 12955) (noting that the "Fair Housing Act prohibits certain forms of discrimination on the basis of race, color, religion, sex, familial status, or national origin" and observing that the "California fair housing law prohibits discrimination on the basis of sexual orientation, marital status, . . . ancestry, . . . source of income, or disability").
276. Id. at 1162.
277. Id.
278. Id. at 1163.
objectionable material to further its policy of protecting children. The court noted the caption of the immunity provision in § 230(c): Protection from “Good Samaritan blocking and screening of offensive material.”

Citing with approval a Seventh Circuit decision, the court held that “the substance of § 230(c) can and should be interpreted consistent with its caption.” The court stated, “Congress sought to immunize the removal of user-generated content, not creation of content.” In fact, the statute expressly provides for liability claims against information content providers responsible for creating or developing the information content in whole or in part.

The court distinguished Roommates’s online activity from that of a passive conduit. It noted Roommates’s business practices solicited unlawful information by asking unlawful questions. Roommates also bore partial responsibility for creating the subscriber profile. Roommates had not merely created a platform that third parties had abused. Instead, the alleged illegality of the site was linked directly to Roommates’s active participation in developing the questions and its search mechanism. The court noted that “[p]roviding immunity every time a website uses data initially obtained from third parties would eviscerate the exception to § 230 for ‘develop[ing] unlawful content ‘in whole or in part.’”

In Federal Trade Commission v. Accusearch Inc., the Court of Appeals for the Tenth Circuit also denied § 230 immunity to an ISP because it was an information content provider. The ISP, Accusearch, used an Internet site to sell personal information, including telephone records. The Federal Trade Commission (FTC) filed suit, alleging Accusearch’s sale of the telephone records “constituted an unfair practice in violation of § 5(a) of the Federal Trade Commission Act (FTCA)." The FTC sought the

280. Id. at 1163–64.
282. Roommates.com, 521 F.3d at 1164 (citing Chi. Lawyers’, 519 F.3d at 666).
283. Id. at 1163 (emphasis in original).
284. Id. (citing § 230(f)(3)).
285. Id. at 1166–67.
286. Id. at 1172.
287. Id. at 1171.
288. FTC v. Accusearch, 570 F.3d 1187, 1197–1200 (10th Cir. 2009).
289. Id. at 1190.
290. Id.
cessation of “Accusearch’s sale of confidential information and to require it to disgorge its profits” from prior sales.”

Appealing the district court’s grant of summary judgment in favor of the FTC, Accusearch claimed § 230 immunity. In response, the Tenth Circuit noted that § 230’s immunity defense only could be granted by showing the defendant is a “provider or user of an interactive computer service,” had acted as a “publisher or speaker,” and had received the relevant information from another provider. The court found Accusearch was, indeed, a content provider because “[b]y paying its researchers to acquire telephone records, knowing that the confidentiality of the records was protected by the law, it contributed mightily to the unlawful conduct of its researchers.” Thus, the court rejected Accusearch’s contention that its activity was neutral, holding instead that Accusearch acted with intent to generate unlawful content. Consequently, CDA immunity did not apply.

According to the Court of Appeals for the Ninth Circuit, § 230 bars claims treating intermediaries as publishers or speakers of third-party content. When, however, a plaintiff’s claim is based on promissory estoppel and not premised on treating the intermediary as a speaker or publisher, § 230 does not bar the claim. In reaching this decision, the court declined to resolve the dispute arising from the Zeran court’s conclusion that “distributor liability is merely a subset of publisher liability for purposes of defamation law.” The defendant sought immunity based solely on § 230(c)(1).

In its reading of the statutory text, the court concluded that “it appears clear that neither this subsection nor any other declares a general immunity from liability deriving from third-party content[.]” Quoting a decision from the Court of Appeals for the Seventh Circuit, the court observed that “[s]ubsection (c)(1) does not mention immunity or any

291. Id.
292. Id.
293. Id. at 1196.
294. Id. at 1200.
295. Id. at 1200-01.
296. Id. at 1201.
297. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1107-09 (9th Cir. 2009).
298. Id. at 1109.
299. Id. at 1104. The court commented that the various parts of § 230 must be read as a whole, which ultimately leads to the conclusion that plaintiff’s state law negligent undertaking claim is barred. Id. at 1105, 1109.
300. Id. at 1100.
301. Id.
synonym.” In fact, the Seventh Circuit “questioned whether § 230(c)(1) creates any form of ‘immunity.’” Moreover, the Seventh Circuit inquired, “[w]hy should a law designed to eliminate ISPs’ liability to the creators of offensive material end up defeating claims by the victims of tortious or criminal conduct?”

As noted, the majority of federal district and state courts have followed the Fourth Circuit’s opinion in Zeran to hold ISPs immune from liability for third-party content. However, Barrett v. Rosenthal, a California Court of Appeal decision, offered a well-reasoned opinion to the contrary. Barrett involved an appeal from an order granting a motion to dismiss a complaint for “libel, libel per se and conspiracy as a strategic lawsuit against public participation” under California’s anti-Strategic Lawsuits Against Public Participation (SLAPP) statute. Barrett concerned two physicians who were nationally recognized consumer advocates, each of whom maintained an Internet website. They had developed these sites to provide, among other things, consumer health guides and to expose “health frauds and quackery.” The physicians alleged the defendant “posted 10,900 messages to newsgroups—an average of 15 per calendar day.” During a two-year period, “one or both of them were mentioned in more than 200 of these messages, all of which were intended to injure their reputations.

The physicians filed a complaint alleging libel per se, libel, and conspiracy against the authors of the posts, which included an alternative

302. Id. (quoting Chi. Lawyers’ Comm., Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008)) (internal quotation marks omitted).

303. Chi. Lawyers’, 519 F.3d at 669 (citing Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003)).

304. Id. at 670; Doe v. GTE Corp., 347 F.3d at 660.


306. Barrett, 9 Cal. Rptr. 3d at 146. A court must engage in a two-step process to determine whether the lawsuit is a SLAPP. Id. at 147. The first step is to assess “whether to demonstrate that the act or acts of which the plaintiff complains were taken ‘in furtherance of the [defendant]’s right of petition or free speech under the United States of California Constitution in connection with a public issue.’” Id. (citing Equilon Enterprises v. Consumer Cause, Inc., 29 Cal. 4th 53, 67 (2002)). If this threshold requirement is satisfied, the second step is for the plaintiff to show a probability of prevailing on the merits of his or her claim. Id.

307. Id. at 144. The physicians involved were Stephen J. Barrett, M.D., and Terry Polevoy, M.D. Id. at 143.

308. Id.

309. Id. at 145.

310. Id.
medicine advocate and director of the Humantics Foundation for Women, as well as several additional defendants. The complaint alleged that the defendants had posted repeated messages defaming them on various online sites, including “two Usenet ‘newsgroups,’ which focused on ‘alternative medicine.’” The trial court struck the complaint as a SLAPP.

Although the trial court found that the online statements falsely accused the physician of engaging in criminal conduct and inappropriately sought to initiate professional disciplinary proceedings or a criminal investigation against the physician, the court provided three reasons for its conclusion that the physician was unlikely to prevail on his claim. The first reason was that § 230 shielded the defendant from liability because she merely republished the online statements and did not create them. Second, plaintiffs alleging public-figure defamation have the burden of proving “actual malice,” which the physician failed to meet. Third, the trial court found that the plaintiffs “could not establish that they suffered monetary damage of any kind.”

On appeal, the California Court of Appeal stated that the Internet is “the most participatory form of mass speech yet developed” and agreed with the trial court’s determination that Internet communications are in a public forum subject to SLAPP. However, the court of appeal disagreed that one of the physicians would be unlikely to prevail on their defamation claims. The court set aside the trial court’s determination on the issues of the § 230 immunity defense, actual malice, and damages, concluding that one of the physicians “was not required to plead special damages, as the republished statement was libelous per se.” The court distinguished the liability rules that apply to primary publishers, distributors, and

311. Ilene Rosenthal was one of several defendants. Id. at 143.
312. Id. at 144. The additional defendants were not involved in the appeal. Id. at 145 n.3. Additionally, the physicians’ lawyer, a named plaintiff in the case, filed a motion to voluntarily dismiss Rosenthal. Id. at 145.
313. Id. at 144.
314. Id. at 143–44.
315. Id. at 142, 150.
316. Id. at 142.
317. Id. at 150.
318. Id.
319. Id. at 149.
320. Id. at 149–50.
321. Id.
The court also briefly examined the legislative history of § 230. The court of appeal next considered Zeran, the leading case construing § 230. The court observed that “[t]he most consequential aspect of the Fourth Circuit’s opinion in Zeran is its conclusion that § 230 immunized providers and users of interactive computer services from liability not only as primary publishers but also as distributors.” To determine the status of the ISP, Zeran focused “solely on section 577 of the Restatement (Second) of Torts,” which states that “[p]ublication of defamatory matter is its communication intentionally or by a negligent act to one other than the person defamed.”

The Barrett court rejected Zeran’s broad immunity conclusion. It held that Zeran completely “ignored the complementary common law rule described in section 581(1) of the Restatement, which is that ‘one who . . . transmits defamatory matter published by a third person is subject to liability if, but only if, he knows or has reason to know of its defamatory character.’” Under Zeran, ISPs enjoy complete § 230 immunity, “despite the fact that the provider or user knowingly distributes defamatory materials, even if the provider or user profits from such conduct.” The court of appeal commented that Zeran’s expansive construction and application of § 230 has caused one trial court judge to have “gagged on the unfairness that resulted from application of such a broad immunity.”

The court reasoned that Zeran was based upon two critical, but faulty, determinations. The first is “that the word ‘publisher’ in § 230(c)(1) refers not just to primary or original publishers of a third-party defamation but also to distributors.” The second is “that confining the immunity to

322. Id.
323. Id. at 151–53.
324. Id. at 152.
325. Id. at 153 (emphasis in original).
326. Id.; Restatement (Second) of Torts § 577 (1974).
327. Id. at 155.
328. Id.
329. Id. (citing Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998)). The court of appeals in Barrett stated that “[s]ince the decision in Zeran, no court has subjected a provider or user of an interactive computer service to notice liability for disseminating third-party defamatory statements over the Internet, though a three-judge minority of the Florida Supreme Court would have done so.” Id. at 153.
330. Id. at 153 (citing Doe v. AOL, 783 So. 2d 1010, 1018 (Fla. 2001) (Lewis, J., dissenting)).
331. Id.
332. Id.
primary publishers would not accomplish the policies section 230 was
designed to effectuate.”333 The court of appeal found no justifiable basis to
apply broad immunity under either determination.334

The court of appeal likewise reasoned that “[l]egislative use of the
legally uncertain word ‘publisher’ is simply too flimsy a basis upon which
to grant providers and users of interactive computer services what amounts
to an ‘absolute protection’ requiring the ‘total sacrifice of the competing
value served by the law of defamation’ and the subordination of ‘a concept
at the root of any decent system of ordered liberty.”335 After all, both
courts and scholars distinguish between publishers and distributors, and
many “eminent law professors writing scholarly articles in learned journals
commonly use the word ‘publisher’ to refer only to a primary publisher,
even when their subject is the transmission of speech in cyberspace.”336 It
is a well-established principle of law “that statutes which invade the
common law... are to be read with a presumption favoring the retention
of long-established and familiar principles, except when a statutory
purpose to the contrary is evident.”337

Ultimately, the court held that the trial court erred in its determination
that § 230 provided absolute immunity to the plaintiffs’ defamation
claims.338 The court found further that “the statute cannot be deemed to
abrogate the common law principle that one who republishes defamatory
matter originated by a third person is subject to liability if he or she knows
or has reason to know of its defamatory character.”339 Therefore, § 230
immunity does not apply to distributors, and did not bar the remaining
plaintiff’s defamation claim.340

Despite the sound and thorough analysis by the court of appeal, the
California Supreme Court adopted Zeran’s rationale, holding that
Congress did not intend to create an exception from § 230 immunity for
distributors.341 Although the Supreme Court stated that it shared the

333. Id.
334. Id.
335. Id. at 157 (citing Gertz v. Robert Welch, Inc., 418 U.S. 323, 341 (1974)).
336. Id. (citing David R. Sheridan, Zeran v. AOL and the Effect of Section 230 of
the Communications Decency Act Upon Liability for Defamation on the Internet, 61
ALB. L. REV. 147, 169-170 n.143 (1997); see, e.g., Cass R. Sunstein, The First
Amendment in Cyberspace, 104 YALE L.J. 1757, 1801 (1995)).
337. Barrett, 9 Cal. Rptr. 3d at 155.
338. Id. at 155-56.
339. Id. at 152 (citing RESTATEMENT (SECOND) OF TORTS § 581(1) (1974))
(emphasis in original).
340. Id. at 167.
concerns of those who have expressed reservations about the Zeran court’s broad interpretation of §230 immunity, as well as the “disturbing implications” such “blanket immunity” provides, the court nonetheless concluded that ISPs are exempt from liability for republication of defamatory statements. As the Barrett court observed, numerous scholars have been critical of the Zeran court’s flawed analysis. In Barrett, the court cited with approval dozens of scholarly articles offering a critical analysis of Zeran. Nearly a decade later, the number of articles critical of Zeran has substantially increased. These scholars provide a well-reasoned basis for

342. Id. at 529.
343. Id.
344. Barrett, 9 Cal. Rptr. 3d at 154.
346. See, e.g., Christina Carmody Tilley, supra note 219, at 121 (arguing that Ninth Amendment “dignitary rights are protected from the diminishment that necessarily follows from an expansive reading of the First Amendment”); Catherine R. Gellis, 2013 State of the Law Regarding Internet Intermediary Liability for User-Generated Content, 69 BUS. LAW. 209 (Nov. 2013); Laura A. Heymann, The Law of Reputations and the Interest
Congress to revisit the injustice created by the Zeran court’s overly broad construction of § 230. While revisiting the issue, Congress also should consider that its “expressed desire to overrule Stratton Oakmont, the absence of any apparent intent to disturb the effect of the decision in Cubby, and the statements of Representative Cox, the author of § 230, are consistent with exclusion of distributor liability from statutory immunity.” Several district courts already have followed suit, concluding that § 230 immunity does not apply for various reasons, including that the ISP was not a publisher or that the ISP was a content provider.

IV. PROPOSED CHANGES
A. DIGITAL MILLENNIAL COPYRIGHT ACT (DMCA)

When Congress enacted the CDA, it was concerned with the ease of access to a nearly limitless electronic universe of information and therefore sought to restrict online access to pornography and other objectionable materials. Section 230(e)(2) of the CDA, however, provides that “[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property.” Ease of online user access and duplication of copyright-protected works creates potential liability for ISPs. In dealing with claims of online infringement of intellectual property, the ISPs find themselves in the same situation as when allegations of online defamation arise. As in defamation cases, the readily identified ISPs, rather than the anonymous or pseudonymous offending users, are more likely to be sued for copyright infringement. For that reason, Congress’ response to the problem of online infringement in the DMCA provides guidance in how online defamation also might be handled.

of the Audience, 52 B.C. L. REV. 1341 (2011); Felix T. Wu, Collateral Censorship and the Limits of Intermediary Immunity, 87 NOTRE DAME L. REV. 293 (2011) (acknowledging the chilling effect of collateral censorship and arguing for limits on intermediary liability when it acts as an original speaker or the type of liability specifically targets intermediaries).

347. Barrett, 9 Cal. Rptr. 3d at 160.
349. See e.g., 141 CONG. REC. 15503 (1995)
351. Stephen A. Hess, Minesweeping the Digital Millennium Copyright Act “Safe Harbors,” COLO. LAWYER, Oct. 2004, at 95 (observing that ISPs are not only more accessible, but also likely more solvent “than the primary infringers”).
In 1998 Congress enacted the DMCA in part to protect copyrighted “works susceptible to being stored and disseminated through the Internet.” The DMCA’s primary goal, protecting authors’ private interests in their creative works, contrasts sharply with that of the Copyright Act, which protects the public’s interests in use and access to copyrighted works.

The DMCA defines a “service provider” in two different ways. Subparagraph (A) defines a service provider as “an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.” The definition of a service provider in subparagraph (B) is broader. It states that a service provider “means a provider of online services or network access, or the operator of facilities therefor, and includes an entity as defined in subparagraph (A).”

Congress established four limitations in the DMCA to address concerns about potential financial consequences of service provider liability on the Internet. These limitations are known as “safe harbors.”

352. Id. Additionally, “Congress enacted the DMCA in 1998 in order to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty (‘WIPO’).” Ross Alexander, Legislative Reform of the Copyright Act’s Fair Use Clause: Failure to Vault Conflict and Express Preemption of the Copyright Act Requires Legislative Attention, 59 SYRACUSE L. REV. 331, 355 (2008). Under WIPO, contracting nations are required “to provide legal protection and remedies ‘against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.” Id. (citing World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty, art. 11, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 2186 U.N.T.S. 152).

353. Alexander, supra note 352, at 355.

354. 17 U.S.C. § 512(k)(1) (2012); see also Richard Belsky, The Digital Millenium Copyright Act And You: A Framework For A Functional Future, 14 U. BALT. INT’L L. J. 1, 46 (2005) (arguing that judicial review of DMCA claims “utilize the functionality framework as a limiting and coordinating doctrine under which undeserving DMCA claims may be filtered out . . . to protect consumers and aftermarket industrialists alike from the potential evils of DMCA overuse); see also Maura L. Rees, Ensuring Qualification For DMCA Section 512(C), in MANAGING INTELLECTUAL PROPERTY ISSUES IN CYBERSPACE 91, 98 (2012), available at 2012 WL 2244968 (providing brief summary of DMCA with recommendations on advising clients concerning the Act).

355. § 512(k)(1)(A).

356. § 512(k)(1)(B); see also Hess, supra note 351, at 95–96.

357. Hess, supra note 351, at 95.
safe harbor provisions in subsections (a) through (d) provide protection from liability for the online activities of third parties, so long as the statutory requirements of the Act are met.359 The provisions state that “[w]hether a service provider qualifies for the limitation on liability in any one of the [safe harbor] subsections [is] based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.”360

The first safe harbor offers protection from liability arising from “transitory digital network communications.”361 The statute provides immunity to an ISP

for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections.362

There are several requirements for this safe harbor. The ISP must not have initiated or directed the transmission of the infringed material. Nor can the ISP select the material or recipients of the material, except in an automated response at the request of another individual.363 The first safe harbor also prohibits an ISP from maintaining a copy of the material on its system or network “in a manner ordinarily accessible” to one other than the intended recipients.364 Moreover, the ISP can maintain the copy for no “longer period than is reasonably necessary for the transmission, routing, or provision of connections.”365 Finally, the ISP shall not modify the content of the materials.366

358. Id. The limitations are set forth in Title II of the DMCA, which is the Online Copyright Infringement Liability Limitation Act (OCILLA), amending the Copyright Act, at 17 U.S.C. § 512.

359. § 512(n). Subsection (n) governs construction of the limitations and provides that the limitation in subsection (a) through (d) offer separate and different limitations that are available to service providers.

360. § 512(n).

361. § 512(a).

362. Id.

363. § 512(a)(1)–(3).

364. § 512(a)(4).

365. Id.

366. § 512(a)(5).
The second safe harbor concerns protection from liability for system caching.\textsuperscript{367} It does not, however, immunize against infringing materials passing through the site.\textsuperscript{368} Many of the provisions governing caching are very similar those in the first safe harbor, with a few notable additions.\textsuperscript{369} For example, in addition to the different definition for service provider, subsection (b) requires a service provider to comply with its own conditions concerning access to cached materials.\textsuperscript{370} Importantly, subsection (b) includes a take-down notice provision. This protects the ISP from liability for providing access to infringing materials if “the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement.”\textsuperscript{371} The take-down notice provision requires the removal of the infringing material from the originating site and confirmation of such removal by the party giving the notification.\textsuperscript{372} Service providers that take down the infringing materials are immune to liability if they meet the other conditions in the system caching provision.\textsuperscript{373}

The DMCA’s third safe harbor relates to “information residing on systems or networks at direction of users.”\textsuperscript{374} Congress recognized the increased potential for infringement liability accompanying website users storing and providing public access to uploaded information on service providers’ sites. Accordingly, “the DMCA imposes obligations on the service providers to eliminate access to infringing materials of which they are given proper notice.”\textsuperscript{375} Therefore, an essential factor in determining whether immunity is available under this safe harbor is whether the service provider had actual or constructive knowledge of the infringing material.\textsuperscript{376}

The notification provisions in the third safe harbor are more extensive than those found in the second safe harbor.\textsuperscript{377} As a result, the provisions in this subsection impose a greater burden on the service provider to earn

\begin{footnotesize}
\begin{enumerate}
\item[367.] § 512(b).
\item[368.] Hess, \textit{supra} note 351, at 97.
\item[369.] § 512(b).
\item[370.] See § 512(b)(2)(B)–(C). “[C]aching refers to creating temporary caches of material to make for more efficient operation of [a] network,” which is distinguished from “hosting [which] refers to storing information.” \textsc{Organisation for Economic Co-operation and Development (OECD)}, \textit{supra} note 49, at 11.
\item[371.] § 512(b)(2)(E) (emphasis added); \textit{see also} Hess, \textit{supra} note 351, at 97.
\item[372.] \textit{See} § 512(b)(2)(E)(i)–(ii).
\item[373.] \textit{See} § 512(b)(2)(E).
\item[374.] § 512(c).
\item[375.] Hess, \textit{supra} note 351, at 97.
\item[376.] \textit{See} § 512(c)(1)(A)(i)–(iii); \textit{see also} Hess, \textit{supra} note 351, at 97–98.
\item[377.] \textit{See} § 512(b)–(c); \textit{see also} Hess, \textit{supra} note 351, at 97–98.
\end{enumerate}
\end{footnotesize}
immunity for the infringing material. For example, the service provider is required to designate and make known to the public an authorized agent to receive notice of potentially infringing material. Likewise, the service provider must list contact information for the agent and any other information “the Register of Copyrights may deem appropriate.”

The DMCA also includes specific procedures the complaining party must follow when notifying the ISP of infringement under the third safe harbor provision. The notice must be in writing, with a “physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is alleged infringed.” The notice also must sufficiently identify the infringed materials to permit removal or disable access to the materials. The notification must contain physical and electronic contact information for the complaining party. Further, the notification must include statements that the use of the alleged infringed materials was unauthorized, the statements in the notice are accurate, and the complaining party is authorized to act on behalf of the owner of the allegedly infringing materials.

The fourth and final safe harbor governs the use of information location tools. Information location tools relate to devices used to refer or link “users to an online location containing infringing material or infringing activity … including a directory, index, reference, pointer, or hypertext link.” Congress included this safe harbor “to ensure that service providers can provide search engines without fear of liability for facilitating the acquisition or propagation of infringing materials that are located on servers over which they have no control.” This final safe harbor also contains a notice and take-down provision.

Therefore, the DMCA expressly incorporates notice and take-down provisions in three of its four safe harbor provisions. Service provider liability turns on notice. After all, service providers with actual or constructive knowledge of allegedly infringing materials have a duty to remove or disable access to the infringing materials to avoid liability.

378. See id.
379. See § 512(c)(2).
380. Id.
381. § 512(c)(3)(A)(i).
382. See § 512(c)(3)(A)(ii)–(iii).
384. See § 512(d).
385. Id.
386. Hess, supra note 351, at 99.
387. See § 512(d)(3).
B. COURTS SHOULD CONSTRUE THE CDA MORE NARROWLY

Numerous courts’ facile adoption of Zeran’s overly expansive application of § 230 immunity to ISPs has largely stripped away individuals’ rights to sue ISPs for defamation by third parties. These courts have failed to distinguish between publishers and distributors. In so doing, courts have ignored the different standards of review that each status invokes. Moreover, in construing § 230 of the CDA, these courts have failed to consider the legislative policies and objectives the statute sets forth. Finally, the courts following Zeran have failed to fully consider what § 230 does and does not state. When these factors are examined, it is apparent that a narrower interpretation of the CDA is warranted as it relates to ISPs and third parties.

In enacting § 230, Congress appears to have attempted to achieve Cubby’s result in cases involving ISPs and improper third party conduct. Congress certainly did not intend to follow what it deemed the “absurd” result of Stratton, which found an ISP liable as a “publisher.” In fact, the legislative history confirms Congressional intent to overrule Stratton. Nothing, however, in the legislative history suggests Congress intended to overrule Cubby, which is specifically mentioned and factually distinguished in Stratton. The court in Cubby determined that CompuServe, the ISP in the case, was a distributor, rather than a publisher. The court equated CompuServe’s editorial control over content on its Internet site to that of such traditional distributors as public libraries, book stores, and newsstands. As a distributor, CompuServe, like its traditional counterparts, could be held liable under traditional state defamation law if it “knew or should have known” of the presence of the defamatory material.

The distinction between “publishers” and “distributors” is important because the caption to § 230(c)(1) is “Treatment of publisher or speaker.” Moreover, § 230(c)(1) expressly provides that “[a] 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.” Yet,

388. Robert Cannon, supra note 167, at 61; see also Freiwald, supra note 1, at 596. See generally H.R. Rep. No. 104-458, at 194 (1996) (Conf. Rep.) (Cox-Wyden Proposal, Chris Cox (R-CA) and Ron Wyden (D-OR)).
393. Id. at 140.
although the statute specifically forbids characterizing ISPs as publishers, it does not state or imply that a provider or user of an interactive computer service may not be treated as a distributor.

In defamation law, the distinction between publishers and distributors is well established. From the language of § 230, one can infer Congressional awareness of this distinction. Given that there is no discussion about distributors in the legislative history or mention in the statutory language, courts should not read § 230 to equate distributors with publishers. Such an expansive reading is particularly indefensible when it virtually eliminates the right of a private individual to seek redress for online defamation involving ISPs acting as distributors. Through this expansive reading, courts effectively grant distributors statutory immunity, even though distributors were not even included in the statute. Congress has not affirmatively fixed this problem.

A narrower reading of § 230 would not give rise to a flood of defamation claims against ISPs acting as distributors. Generally, the standard the plaintiff must meet to prove defamation by a distributor is different from the standard required for publishers. As discussed, a plaintiff must prove the distributor knew or reasonably should have known that the distributed material was defamatory. The plaintiff may prove awareness of the defamatory material by showing that the plaintiff informed the distributor of the defamatory content and the distributor continued to distribute the content. The heightened constitutional standards of New York Times v. Sullivan and Gertz also apply to content relating to matters of public concern. Thus, only with notice of defamatory materials can ISPs face liability for third-party content. As with traditional rules of defamation concerning distributors, once notice of the alleged defamatory content is received, the ISP has a duty to investigate and avoid further harm. Even then, the ISP can escape liability if it takes such action. ISP liability for third-party content applies only if the ISP knew or reasonably should have known of the defamatory content and failed to remove it.

Section 230 of the CDA is commonly referred to as the “Good Samaritan” provision because that term is included in the caption of § 230(c) and because § 230(c) grants immunity to ISPs that, on their own initiative, block or remove offensive content from their sites. Thus, both the title and effect of § 230(c) indicate Congressional intent to protect

394. See, e.g., id. at 139.
395. Id. at 140–41.
ISPs from liability if they voluntarily act to restrict or limit access to offensive material online. The link between “good faith” action and immunity accords with the narrower statutory construction of § 230, which would hold ISPs acting as distributors liable for third-party defamatory content only if they failed in good faith to ameliorate the wrong. This less-expansive view of the CDA remains consistent with the stated policy of protecting children from pornographic and otherwise obscene materials, while promoting self-regulation of the Internet with limited government interference. Holding ISPs liable for third-party defamatory content that the ISP knows or should know is on their sites would not dilute either of these stated goals.

C. CONGRESS SHOULD REVISE § 230 OF THE CDA

Assuming Congress intended to grant general immunity to ISPs for third-party online content, as most courts have determined, Congress now should revise § 230 of the CDA to allow individuals to seek redress under state common law claims and allow state criminal laws to be enforced. Indeed, “[t]here is no reason inherent in technological features of cyberspace why First Amendment and defamation law should apply differently in cyberspace than in the brick and mortar world.” The DMCA provides a model for how defamation law could be handled in an online world. The DMCA conditions ISP liability for online infringement of copyright-protected works on the service provider’s actual or constructive knowledge of infringement. The CDA should be revised along similar lines. If that revision was made, ISPs would enjoy immunity from liability for defamation when, after sufficient notice, they removed defamatory material posted by third parties on their sites. Liability for such third-party defamation would arise only upon the plaintiff’s demonstration that an ISP had actual or constructive knowledge of the defamatory content on its site and had failed to take it down.

396. § 230 serves as a “safe harbor” for provisions of the CDA that have been declared unconstitutional. Consequently, Congress should abolish this immunity provision. “[I]n July 2013, the attorneys general of forty-nine states wrote to Congress requesting that the CDA be amended to expressly state that it does not preempt state criminal statutes.” Stephanie Silvano, Note, Fighting A Losing Battle to Win the War: Can States Combat Domestic Minor Sex Trafficking Despite CDA Preemption?, 83 FORDHAM L. REV. 375, 398 (2014) (emphasis in original).

397. Batzel v. Smith, 333 F.3d 1018, 1020 (9th Cir. 2003) (acknowledging Congressional ‘policy reasons to immunize from liability for defamatory or obscene speech ‘providers and users of interactive computer services’ when the defamatory or obscene material is ‘provided’ by someone else”).

398. Id.
Like the CDA, the DMCA grants immunity to ISPs for information content provided by third parties.\(^{399}\) Unlike the CDA, however, the DMCA “provides specific notice, take-down, and put-back procedures that carefully balance the First Amendment rights of users with the rights of a potentially injured copyright holder.”\(^{400}\) The DMCA provides a process for individuals to protect their interests in copyrighted works. When a copyrighted work is posted on a website, the ISP may not be aware the work is protected. The DMCA’s notice provisions bring the work’s protected status to the ISP’s attention.\(^{401}\) This relieves the ISP of the burden of policing third-party content. Working in tandem with the notice provisions, the take-down provisions allow individuals to seek redress from an ISP that refuses to remove protected work after a reasonable period of time.\(^{402}\) Additionally, the DMCA provisions give the ISP the opportunity to protect itself from liability for posting the copyrighted work without permission.\(^{403}\)

With relatively little tinkering, the CDA could be revised to create a similar scheme related to defamatory content. Indeed, the CDA’s existing provisions relating to obscene material would not even have to be adjusted. The revision would merely require adding a provision listing the actions needed to characterize an ISP as a “distributor,” while differentiating them from an ISP’s actions making them a “publisher.”

A safe harbor provision similar to those in the DMCA could also be added. Such a provision likely would require entities to follow a stipulated form to provide notice of defamatory content to ISPs. Upon receipt of such notice, the ISP would be required to take down the defamatory content within a reasonable time or face liability from the defamed party. Thus, an ISP would be immune once it voluntarily removed third-party defamatory content after appropriate notice.

An additional provision could be added to provide some protection for ISPs that do not take down the material within the stipulated time for removal. Such a provision would require the defamed party to file their defamation claim within a certain number of days after the time for removal had expired, in order to avoid the extinguishment of her claim.

\(^{399}\) Id. at 1032 n.19.
\(^{401}\) See Batzel, 333 F.3d at 1032.
\(^{402}\) Id.
\(^{403}\) Id.
The proposed revision would not affect the CDA’s initial goals of protecting children from online obscenity and empowering parents to block objectionable content. Nor would the revision impose any greater governmental regulation upon ISPs than the CDA already imposes. Indeed, the revision imposes no burden on the ISPs until they receive notice of defamatory content and, even then, it grants them immunity in return for the minimal effort of removing the defamatory material from their sites. It should also be remembered that the ISPs already benefit from the constitutional protections that New York Times and Gertz provide in relation to the communication of public-interest content. What the revision would do, however, is provide relief to individuals who suffer the indignity of having defamatory materials posted online. In providing such relief, the revision imposes upon ISPs no greater burden than that imposed by state defamation law upon their traditional counterparts—the public libraries, newsstands, and booksellers.

There are several criticisms of the DMCA, including its effect on free speech and the potential for abuse in the extrajudicial notice and take-down process. Another criticism is the potential chilling effect of the DMCA in academic and scientific research, particularly for publicly available software. Another criticism of the DMCA is that its anti-circumvention provision “creates new rights that ordinarily would not be afforded copyright owners under the traditional notions of copyright, such as a ‘pseudo-copyright’ in works whose true copyright may not even exist.” Another concern with the DMCA subpoena power is that it does not adequately protect First Amendment interests in anonymous speech. Further criticism is that the burden of monitoring the Internet is placed on the copyright owner who must then provide notice. Additionally, the DMCA process “treats the fair user and the infringing user exactly the

---

same way; it denies both users the opportunity to defend their respective uses before takedown.\textsuperscript{408}

D. INTERNATIONAL LAW AND ONLINE DEFAMATION

As in the United States, many OECD member nations also provide some form of exemption from liability for “ISPs and other information intermediaries who act as middlemen (i.e., merely deliver content) by creating liability exceptions for these entities, e.g., in their e-commerce or copyright laws.”\textsuperscript{409} In the European Union, the European Data Protection Directive affords strong protection for individual privacy.\textsuperscript{410} In a 2014 privacy case originating in Spain, the European Court of Justice (ECJ) essentially determined that its citizens have the right to be forgotten and “ruled that search engines need to remove links to Web results if they contain information an individual deems should be ‘forgotten.’”\textsuperscript{411}

A man filed a privacy suit under Spain’s data protection laws against Google Spain SL and Google, Inc., (collectively, Google) alleging harm to his reputation based on search engine results including ten year old newspaper stories about a real estate auction to settle a debt.\textsuperscript{412} The


\textsuperscript{409} ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), supra note 49, at 10. The OECD report identifies § 230 of the CDA and the DMCA, and states that Australia has “[s]imilar principles on the liability of online intermediaries” regarding violation of copyright law. \textit{Id.} In Korea, ISPs may be exempt from liability under certain circumstances, pursuant to the “Act on Promotion of Information and Communications Network Utilization and Information Protection” and the “Copyrights Act.” \textit{Id.} In Japan and the European Union, respectively, “the Japanese Law of 2001 and the European Electronic Commerce Directive (ECD) of 2000 [were enacted] to establish a liability regime for some types of online intermediary activities.” \textit{Id.} at 11. Intermediary activities include providing, transmitting or storing “by, or at the request of, a recipient of the service” (in other words, the recipients of the service as those who publish information as well as those who access the information). \textit{Id.} The ECD “establishes a horizontal exemption from liability for intermediary information society service providers when they play a technical role as a mere conduit of third party information and limits service providers’ liability for the other intermediary activities of caching and hosting information.” \textit{Id.} (internal quotations omitted). Generally, “mere conduit” is the equivalent of “networks and access provision, ‘caching’ refers to creating temporary caches of material to make for more efficient operation of the network, and hosting refers to strong information.” \textit{Id.} at 11. For the exemption to be available, the “mere conduit” “must have neither knowledge nor control over the information.” \textit{Id.}

\textsuperscript{410} See generally Patrick Van Eecke & Jim Halpert, The Right To Be Forgotten In Today’s Information Age, WESTLAW J. COMPUTER & INTERNET, Nov. 20, 2014, at 1.

\textsuperscript{411} \textit{Id.}

\textsuperscript{412} \textit{Id.} (citing Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. C-131/12 (Judgement of the Court)). “Under the European Data
newspaper declined to block the pages from being indexed by Google’s search engines.\textsuperscript{413} The Spanish reviewing agency concluded that Google must remove the data from their indexing process and make future access to the defamatory material impossible.\textsuperscript{414} The Spanish high court submitted two questions to the ECJ; first, “the applicability of European privacy laws on processing personal data abroad,” and second, “the proper balance between the rights of individuals and search engines under EU’s current privacy legislation.”\textsuperscript{415}

Acknowledging the impact of search engine technology and its “decisive role in the worldwide dissemination of information,” the ECJ held that European privacy laws apply “even if search engine indexing occurs in the United States.”\textsuperscript{416} Specifically, Spain’s privacy laws applied because Google “promotes and sells advertising space in Spain.”\textsuperscript{417} Alternatively, Spanish law could also apply because Google used datacenters, servers, and cookies that stored data “on an EU member state user’s computer.”\textsuperscript{418} While the ECJ was faced with issues largely related to “Internet search engines, the ruling may also have significant consequences for Internet publishers and companies offering Internet-based services, whether they are located inside or outside of Europe.”\textsuperscript{419}

The ECJ’s “right to be forgotten” ruling is a significant departure from the law in the United States, especially in light of § 230 immunity and the First Amendment.\textsuperscript{420} These different jurisdictional outcomes result in

\begin{footnotesize}
\begin{enumerate}
  \item The article describes Google’s indexing process as follows:
    \begin{quote}
      The Web is like an ever-growing public library with billions of books and no central filing system. Google essentially gathers the pages during the crawl process and then creates an index, so we know exactly how to look things up. Much like the index in the back of a book, the Google index includes information about words and their locations. When you search, at the most basic level, our algorithms look up your search terms in the index to find the appropriate pages.
    \end{quote}
  \item Id. at 4 n.2 (quoting Inside Search: Crawling and Indexing, GOOGLE, http://www.google.com/insidesearch/howsearchworks/crawling-indexing.html (last visited April 11, 2015)).
  \item Id. at 1–2.
  \item Id. at 1.
  \item Id. at 2.
  \item Id.
  \item Id.
  \item Id. at 1.
  \item Id. at 4.
\end{enumerate}
\end{footnotesize}
“libel tourism.”\textsuperscript{421} Libel tourism is “a form of international forum shopping for defamation plaintiffs . . . allowing such plaintiffs ‘to benefit from both favorable substantive and procedural law.’”\textsuperscript{422} Libel tourists flock to the United Kingdom because of its notorious pro-plaintiff defamation laws.\textsuperscript{423} The United Kingdom recently enacted the Defamation Act of 2013, which may impact libel tourism, as the Act “rebalances the law in favor of freedom of speech.”\textsuperscript{424} The new law provides defenses for truth and honest opinions, “[r]epositioning the common law defenses of justification and fair comment.”\textsuperscript{425} Recognizing the importance of editorial discretion, the new law also created a new public interest defense.\textsuperscript{426}

Canada’s approach concerning intermediary liability and notice is comparable to the European Union’s Electronic Commerce Directive and its implementing regulations.\textsuperscript{427} In Canada, case law likewise suggests that intermediary liability for online statements created by third parties is based on fault and requires actual or constructive knowledge of the defamatory content.\textsuperscript{428}


\textsuperscript{422} Manzo, supra note 421, at 159.

\textsuperscript{423} See Lee Levine & Stephen Wermiel, \textit{The Landmark That Wasn’t: A First Amendment Play in Five Acts}, 88 WASH. L. REV. 1, 53 n.317 (2013); see also Corey Omer, \textit{Intermediary Liability for Harmful Speech: Lessons from Abroad}, 28 HARV. J.L. & TECH. 289, 298 (2014) (commenting that “the United Kingdom was viewed as an attractive pick for plaintiff forum shoppers due to its flexible jurisdictional requirements and generous libel law”).


\textsuperscript{425} Anthony Lester, supra note 421, at 186.

\textsuperscript{426} \textit{Id.}

\textsuperscript{427} \textit{Id.} at 308–309, 314 (offering a comparative analysis of intermediary liability for user-created content and favoring “international harmonization and reduced reliance on intermediary knowledge, assessment, and monitoring”).

\textsuperscript{428} Corey Omer, supra note 423, at 305 (“To escape liability, an intermediary would have to show that it ha[d] no actual knowledge of an alleged libel, [w]as aware of no circumstances to put [it] on notice to suspect a libel, and committed no negligence in failing to find out about the libel . . . .”) (quoting Soc. of Composers, Authors & Music Publishers of Can. v. Canadian Ass’n of Internet Providers, 2 S.C.R. 427, para. 89 (Can. 2004) (modifications in original)).
The “right to be forgotten” will restrict free speech. As one scholar explained: “[l]iability for noncompliance with the right to be forgotten runs only if one refuses to delete, not if one deletes at the drop of a hat.” He argues that mere negligence in “[r]emoving art and free expression” results in no penalty, while “the liability for failure to delete is fearsome: a fine of up to two percent of [the intermediary’s] annual worldwide income.” Thus, the potential liability pursuant to the European Union right to be forgotten “transforms Facebook, Google, Reddit, and [other intermediaries] into censors, charged with evaluating whether a particular expression has artistic or journalistic merit or otherwise constitutes free expression.”

V. CONCLUSION

When Congress enacted § 230 of the CDA, it essentially eliminated individuals’ ability to recover damages from Internet intermediaries for defamatory statements made by third-party users on the intermediaries’ websites. As enacted and construed by the courts, § 230 is ineffective in its effort to limit access to pornography and other obscenities, and provides little or no incentives for intermediaries to engage in self-monitoring. The power of states to grant relief for reputational harm to its citizens should not yield to an inadequate and ineffective statute. Guided by the notice-based provisions of the DMCA, Congress should revise § 230 of the CDA to include notice and take-down provisions. The revised statute should clarify that intermediaries, as distributors, will be held liable for communicating defamatory material after receiving notice of the defamation. This result is consistent with traditional defamation law, where a distributor or secondary publisher is liable for communications when it has actual or constructive knowledge of defamatory content.

430. Id. at 539 (emphasis omitted).
431. Id.
432. Id.