AMANDA STERLING

DEFAMATION 2.0: UPDATING THE COMMUNICATIONS DECENCY ACT OF 1996 FOR THE DIGITAL AGE

May 25, 2016

Abstract: Twenty years ago, President Bill Clinton signed the Communications Decency Act (“CDA”) into law as Title V of the landmark Telecommunications Act of 1996. The statute restricts the transmission of obscene material on the Internet and, secondarily, defines who is subject to liability for unlawful content posted online. Congress carefully drafted the bill to reflect concerns about the law’s effects on the Internet’s growth and development, and to avoid chilling online speech and activity. The CDA, as enacted, immunizes websites and Internet service providers against liability for republishing tortious and otherwise unlawful content. In doing so, it dramatically departs from the common-law rules that govern defamation liability offline. The Internet of 2016, however, bears little resemblance to the Internet of 1996. The concerns that shaped the CDA no longer justify such a hands-off approach to tortious online speech; and as applied to today’s worldwide web, the statute creates problematic incentives, outcomes, and policy concerns. This Article examines the ways in which the CDA fails to account for critical features of the Internet as the medium has evolved since 1996, and then presents proposals as to how the statute might be updated to better suit the needs of today’s digital age.

DEFAMATION 2.0: UPDATING THE COMMUNICATIONS DECENCY ACT OF 1996 FOR THE DIGITAL AGE

Amanda Sterling

Mr. President, the use of computer networks holds tremendous potential for the expansion of public dialog and discourse advancing the value of the First Amendment. It is an industry that is growing by leaps and bounds.

The business, educational, and social welfare potential of the information superhighway is almost without limit. It would be devastating to limit the potential of this medium by taking steps that could have the effect of silencing its users.

Senator Russell Feingold

INTRODUCTION

When Congress enacted the Communications Decency Act of 1996, the nascent Internet bore little resemblance to the worldwide web that is so deeply engrained in American life today. Around that time, when the Internet had just been opened up to full commercial use, only four percent of the public consumed news online, and only three percent of Internet users had ever

---

3 See Barry M. Leiner et al., A Brief History of the Internet, 39 ACM SIGCOMM Computer Comm. Rev. 22, 27–28 (2009). While the web had previously served as a platform for some private commercial activity, it also had been subject to restrictions designed to preserve the medium for academic, scientific, and military purposes. SHANE GREENSTEIN, DIAMONDS ARE
accessed the worldwide web.\(^5\) The number of sites on the web grew from approximately fifty in 1993 to more than fifty million by the turn of the millennium,\(^6\) and the volume of global Internet traffic jumped from 100 GB per hour in 1997 to more than 16,000 GB per second in 2014.\(^7\) Today, the Internet makes up an enormous—and critically important—part of the media environment, having overtaken traditional media in marketplaces around the globe.\(^8\)

The advent of the Internet age has clearly and inarguably reshaped countless facets of modern life, particularly the ways in which we as a society transmit, create, and consume information.\(^9\) The law, however, has not kept pace with these rapid cultural and technological developments. Defamation law, in particular, has become an anachronism. The provision of the Communications Decency Act that governs defamatory online speech has not been updated or otherwise amended since the statute’s enactment during the relative infancy of the Internet.\(^10\) Given the nature of the Internet’s paradigm shift, the time is ripe to revise this critically out-of-date provision to better reflect the needs of the digital age.

This Article proceeds in four Parts. Part I begins with a short overview of defamation law, first presenting a summary of the common-law framework and

---


\(^7\) *Ctr. for Am. Progress, Power of Progressive Economics: The Clinton Years 8* (2011).


then highlighting the relevant portions of the Communications Decency Act. Part II traces the development of the Internet over the past two decades, placing particular focus on the content that populates the worldwide web and the ways in which that content is created, developed, disseminated, and accessed. Part III examines online defamation law in light of the lessons and technological advances of the last twenty years by looking specifically to the validity of the original policy justifications underlying the statute, the support that these rationales provide for the law today, and cases addressing the scope of the statute. Part IV concludes with a discussion of proposed reforms, each of which would better reflect the policy objectives behind the statute and achieve a more appropriate balance between the many interests implicated by defamatory speech online.

I. THE CURRENT LEGAL LANDSCAPE

A. Offline: Common-Law Framework

The common law of libel evolved in a way that distinguished between publishers and distributors of defamatory content. Publishers could be held liable for communicating defamatory material upon a showing of mere negligence, whereas distributors could be held liable for defamation only upon a showing of fault or culpability, specifically upon a showing that the distributor knew or had reason to know that the material being disseminated was defamatory. However, an exception to this common-law framework developed in the context of broadcast technology. Disseminators of defamatory material over the radio or television—that is, broadcasters—were treated as original publishers, and thus subject to the stricter standard of liability. Thus, the common law of defamation established different standards of liability for publishers and distributors, and provided that the applicable standard would depend in part on the medium through which the defamatory material was communicated.

---

11 See Restatement (Second) of Torts §§ 577, 581 (Am. Law Inst. 1977) (establishing different standards of liability for distributors of libelous content than those applied to publishers). Compare Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135, 140–41 (S.D.N.Y. 1991) (concluding that the defendant was a “distributor” of online content, and thus could not be held liable for the defamatory material it transmitted), with Stratton Oakmont, Inc. v. Prodigy Services Co., No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. 1995) (holding that the defendant was a publisher and thus subject to liability for defamatory content posted on its online bulletin boards), superseded by § 230(c).
12 See Restatement (Second) of Torts § 577.
13 Id. § 581.
14 Id. § 581(2). This exception reflects traditional defamation law principles, adapted to account for relevant differences inherent in modern broadcast media. Id. § 581 cmt. g.
15 Id. § 581(2).
Since the original development of this doctrine, the U.S. Supreme Court has held that the First Amendment imposes certain outer limits on liability for defamation and libel.\textsuperscript{16} Under modern defamation law, private plaintiffs who claim to have suffered injury as a result of a defendant’s defamatory statements must show that the defendant acted negligently in order to recover.\textsuperscript{17} Public officials\textsuperscript{18} and public figures,\textsuperscript{19} in contrast, must show that the defendant acted with “actual malice,” meaning actual knowledge that the defamatory content was false or reckless disregard as to whether or not it was true.\textsuperscript{20} This body of case law also modified the common-law rules with respect to evidentiary standards, burdens of proof, and damages.\textsuperscript{21}

These constitutional developments substantially narrowed the circumstances in which defamation victims can recover.\textsuperscript{22} Prior to \textit{New York Times Co. v. Sullivan}\textsuperscript{23} and its progeny, a private plaintiff could constitutionally bring a defamation suit on a theory of negligence or even strict liability, depending on the applicable state law, against a speaker who had defamed him.\textsuperscript{24} Were the plaintiff able to prove his case by a preponderance of the evidence, he could potentially recover punitive damages unless the defendant could prove the truth of the de-

\textsuperscript{17} \textit{Gertz,} 418 U.S. at 348–51.
\textsuperscript{18} \textit{Sullivan,} 376 U.S. at 279–80.
\textsuperscript{19} \textit{Curtis Publ’g Co.,} 388 U.S. at 154–56 (plurality opinion), \textit{construed in Gertz,} 418 U.S. at 336 (“[A] majority of the Court [in \textit{Curtis Publishing Co.}] agreed with Mr. Chief Justice Warren’s conclusion that the \textit{New York Times} test should apply to criticism of ‘public figures’ as well as ‘public officials.’”); \textit{see also Milkovich v. Lorain Journal Co.,} 497 U.S. 1, 14–15 (1990) (describing this doctrinal development).
\textsuperscript{20} \textit{Sullivan,} 376 U.S. at 279–80.
\textsuperscript{21} \textit{Id.} at 260, 267, 285–86; \textit{see also Gertz,} 418 U.S. at 340–41; \textit{Milkovich,} 497 U.S. at 16, 21 n.8.
\textsuperscript{23} 376 U.S. 254.
\textsuperscript{24} \textit{Gertz,} 418 U.S. at 342 (identifying “the common-law rule of strict liability for libel and slander”).
famatory material. Post-\textit{Sullivan}, the plaintiff must demonstrate that the defendant was at least negligent; he bears the burden of proving that the material in question was false, at least where the speech is on a matter of public concern; and he cannot recover punitive damages unless the defendant acted with actual malice. Despite this doctrinal evolution, however, the basic distinction between publishers and distributors remains intact—at least with respect to offline communications—and thus this framework continues to govern in cases involving television, radio, or print media.

\textbf{B. Online: The Communications Decency Act of 1996}

Today, the question of liability for defamatory content published online is governed by § 230 of the Communications Decency Act of 1996 (“CDA”). The CDA was primarily designed to restrict children’s access to online pornography, a problem that attracted considerable attention and alarm as the Internet entered mainstream American life. The original version of the bill did not protect providers of Internet services from liability for disseminating content created by their users; § 230 was added as an immunity provision for those providers only after the legislation had been referred to the House. The U.S. Supreme Court struck down the CDA’s core anti-indecency provisions as unconstitutional shortly after the bill became law, but § 230 continues today in force.

Section 230 breaks sharply from the common law of defamation. It immunizes “interactive computer service” providers and users from liability for defamatory and other unlawful content “provided by another information content provider.” The CDA thereby redraws the critical line—for purposes of liability for defamation—between “information content providers” and “interactive com-

\begin{itemize}
\item \textit{Id.} at 340–41, 346.
\item \textit{Id.} at 347–50.
\item \textit{Gertz}, 418 U.S. at 350.
\item \textit{Restatement (Second) of Torts} div. 5, chs. 24–27, special note (\textit{Am. Law Inst.} 1977).
\item S. 652, 104th Cong. (1995).
\item 47 U.S.C. § 230(c) (2014).
\end{itemize}
puter service” providers and users. The statute also immunizes interactive computer service providers from liability based on their good-faith attempts to restrict the availability of “objectionable” material. Section 230’s grant of immunity is broad, perhaps especially in that it preempts inconsistent state laws. However, there is a carve-out that specifies that interactive computer service providers remain subject to liability under federal criminal or intellectual property laws.

The text of § 230 indicates that the provision was intended to (1) minimize governmental regulation of free speech on the Internet, thereby avoiding any potential inhibition of the development of the worldwide web due to the specter of liability, and (2) create an environment in which market actors would self-regulate. Courts have explicitly recognized and drawn upon these two basic policy considerations in applying § 230 and navigating the new field of defamation law in the Internet age. Some have also observed the fact that an alternative

36 See Zeran v. Am. Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997) (holding that § 230 precluded AOL from being held liable, whether as a publisher or distributor, for defamatory content posted through its services); see also, e.g., Jones v. Dirty World Entm’t Recordings LLC, 755 F.3d 398, 407 (6th Cir. 2014) (“Section 230 marks a departure from the common-law rule that allocates liability to publishers or distributors of tortious material written or prepared by others.”). “Interactive computer service” providers, for purposes of the statute, include “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.” § 230(f)(2). As interpreted by the courts, this immunizes both websites (like AOL or Craigslist) and providers of Internet telecommunications services (like Verizon). See Zeran, 129 F.3d at 331–32; see also Jones, 755 F.3d at 407.

37 See RESTATEMENT (SECOND) OF TORTS § 581 (AM. LAW INST. 1977) (establishing different standards of liability for distributors of libelous content than those that applied to publishers).

38 § 230(c)(2)(A).

39 Id. § 230(e)(3).

40 Id. § 230(e)(1)–(2). Section 230 also explicitly exempts liability under the communications privacy law from its grant of immunity. Id. § 230(e)(4).

41 See id. § 230(b)(1); see also Zeran, 129 F.3d at 330–31.

42 See § 230(b)(4). Section 230 was expressly intended to supersede cases such as Stratton Oakmont, Inc. v. Prodigy Services Co., No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. 1995), in which the Supreme Court of New York held that a website was liable as a publisher under traditional defamation law because it exercised editorial control over the material posted on its online bulletin board. See 141 CONG. REC. 22,025 (1995) (statement of Rep. Cox); see also Zeran, 129 F.3d at 330–31.

43 See, e.g., Batzel v. Smith, 333 F.3d 1018, 1027 (9th Cir. 2003) (looking to the “two primary reasons” for the addition of section 230 to the CDA); Ben Ezra, Weinstein & Co. v. Am. Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000) (observing that Congress wanted to create an environment in which websites and service providers could self-regulate); Zeran, 129 F.3d at 330–31 (outlining the policy-based goals behind § 230); Barrett v. Rosenthal, 146 P.3d 510, 517 (Cal. 2006) (recognizing
liability rule could create the risk of a “heckler’s veto” by which private parties could censor speech and impose serious burdens on websites and service providers simply by complaining about content that had been posted online.\textsuperscript{44}

In light of these explicit policy considerations, courts that have reviewed the scope of § 230 have construed the statute liberally and concluded that the question of whether an online publisher can be held liable for allegedly defamatory material turns on whether the publisher actively participated in creating or developing the defamatory content.\textsuperscript{45} As courts have applied and elaborated upon the doctrine, it has become clear that an interactive computer services provider will not be deemed to have contributed to such creation or development unless he has in some way actively contributed to the creation of the unlawful aspect of the content itself.\textsuperscript{46} Indeed, the Sixth Circuit recently suggested that a website that provides a forum for third-party posting will not be responsible for “creating or developing” content, and thus will be entitled to section 230 immunity, unless the website (1) posts legally problematic content itself, (2) compensates third parties for posting legally problematic content, or (3) “require[s] users to violate the law as a condition of posting.”\textsuperscript{47} Thus, § 230 immunity sweeps very broadly, eviscerating the common-law distinction between distributors and publishers\textsuperscript{48} online
and allowing liability to be imposed only in a narrow subset of situations in which the website or service provider logically could be considered a co-creator of the defamatory portion of the objectionable content.\textsuperscript{49}

II. INTERNET REVOLUTION

In the two decades since the CDA became law, rapid advancements in technology have facilitated similarly dramatic developments in information creation, publication, transmission, and consumption on the Internet.\textsuperscript{50} Part II sketches these aspects of digital content’s evolution before proceeding to explain, in Part III, why such developments have significant implications for the CDA as a matter of policy.

A. The Context: The Web in 1996

The modern form of the Internet was unforeseen, and perhaps unforeseeable, when the CDA was enacted. The Internet was originally conceived of as a network for research and educational purposes rather than commercial ends;\textsuperscript{51} prior to the mid-1990s, the federal government controlled the core network infrastructure.\textsuperscript{52} It was not until April 1995 that the Internet became fully open to commercial use,\textsuperscript{53} and early proponents and users of the Internet greeted the possibility of commercialization with some suspicion.\textsuperscript{54} Nevertheless, the web rapidly shifted from an education-oriented medium to a commercial platform in the latter half of the decade, after the final restrictions on commercial use were re-immunizes distributors from liability); \textit{Barrett}, 40 P.3d at 513 (“We conclude that § 230 prohibits ‘distributor’ liability for Internet publications.”).

\textsuperscript{49} See \textit{Roommates.com, LLC}, 521 F.3d at 1168 (“[A] website helps to develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct.”); see also \textit{Accusearch, Inc.}, 570 F.3d at 1200 (adopting the Ninth Circuit’s \textit{Roommates.com} test in determining whether the defendant could claim immunity under § 230).

\textsuperscript{50} See, e.g., \textit{Benkler, supra} note 9, at 1 (“The change brought about by [the Internet revolution] is deep. It is structural. It goes to the very foundations of how liberal markets and liberal democracies have coevolved for almost two centuries.”); Ashraf Darwish & Kamaljit I. Lakhtaria, \textit{The Impact of the New Web 2.0 Technologies in Communication, Development, and Revolutions of Societies}, 2 J. ADVANCES INFO. TECH. 204, 213–14 (2011) (examining the importance from a global perspective of the shift from Web 1.0 to Web 2.0).

\textsuperscript{51} See Leiner et al., \textit{supra} note 3, at 29.


\textsuperscript{53} Leiner et al., \textit{supra} note 3, at 28.

moved. The domain name system—a crucial component of the Internet’s infrastructure—was not formalized until 1998, and some expressed concern about the implications that commercial use would have for the Internet’s identity.

By the time the government permitted complete commercial use and enacted the CDA, hundreds of millions of public-sector dollars had been devoted to the development of the Internet, a consequence of the U.S. government’s substantial investments in computer science research for two full decades prior to this privatization. Laws and regulations were consciously structured to promote the Internet’s rapid development and proliferation, and with barriers to commercialization fully removed, venture capitalists poured billions of dollars into Internet-related commercial investments. This influx of capital provided the opportunity for significant evolution and growth and eventually helped the Inter-

55 See Mowery & Simcoe, supra note 52, at 1379 (discussing “[t]he speed and magnitude of the shift in the Internet from a research network to a commercial opportunity”). Prior to 1995, the government had restricted purely commercial Internet activity as an “unacceptable use” of the technology. See, e.g., Nat’l Sci. Found., The NSFNET Backbone Services Acceptable Use Policy §§ 10–11 (1992) (explicitly articulating these restrictions).


57 See, e.g., Greenstein, supra note 54, at 152 (discussing concerns about whether the Internet might be “unsuitable” for commercial use); Leiner et al., supra note 3, at 31 (“We now see, in the debates over control of the domain name space and the form of the next generation IP addresses, a struggle to find the next social structure that will guide the Internet in the future. . . . If the Internet stumbles, it will not be because we lack for technology, vision, or motivation. It will be because we cannot set a direction and march collectively into the future.”).

58 Mowery & Simcoe, supra note 52, at 1383.

59 Id.; see also, e.g., Office of the White House Press Sec’y, Remarks by the President at a Campaign Event in Roanoke, Virginia (July 13, 2012) (“The Internet didn’t get invented on its own. Government research created the Internet so that all the companies could make money off the Internet.”).

60 Mowery & Simcoe, supra note 52, at 1384 (“In addition to supporting Internet-related R&D, the U.S. government influenced the development and diffusion of the Internet through regulatory, antitrust, and intellectual property rights policies. The overall effect of these largely uncoordinated policies was to encourage rapid commercialization of Internet infrastructure, services and content by new firms.”); see also Fed. Commc’ns Comm’n, Office of Plans & Policy, OPP Working Paper No. 29, Digital Tornado: The Internet and Telecommunications Policy, at i (1997) (“Limited government intervention is a major reason why the Internet has grown so rapidly in the United States. The federal government’s efforts to avoid burdening the Internet with regulation should be looked upon as a major success, and should be continued.”); Ev Ehrlch, Progressive Policy Inst., A Brief History of Internet Regulation 1–14 (2014); Leiner et al., supra note 3, at 27–28.

When the CDA was enacted in 1996, however, this technology existed at a crossroads: the Internet was poised to become the “information superhighway” that many believed it should be, but there was no hard-line guarantee that the medium would make good on its promise.

B. The Evolution: The Internet Since the Enactment of the CDA

One of the most important developments during the late 1990s and early 2000s, separate and apart from Internet technology, involved online content and the way that this material is created, shared, consumed, and discussed. While the Internet’s transformation certainly involved technological developments, it was not solely an infrastructure-driven movement. Rather, the transformation into the modern web is best understood as a change in the zeitgeist of the Internet around the turn of the millennium, or as a shift in the “gravitational core” of Internet use. This development has been the subject of much scholarly discussion and has been described by various experts in the field as an evolution from “Web 1.0” to “Web 2.0,” from “packaged goods media” to “conversational media.”

---

62 See Brett Frischmann, Privatization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Market, 2 Colum. Sci. & Tech. L. Rev. 1, 20–21 (2001) (“Between 1995 and 2000, private investors poured a tremendous amount of resources into all sorts of Internet-related ventures, ranging from infrastructure to applications. Consequently, the NSFNET blossomed into the Internet as we know it today . . . .”).


64 See Greenstein, supra note 54 (examining the many factors, some predictable and some simply lucky, that contributed to the success of the commercialization of the Internet).


66 Dwivedi et al., supra note 65, at 5.


and from an “industrial information economy” to a “networked information economy.”

Because the Web 1.0/2.0 terminology is perhaps most familiar in common parlance, this Article adopts it to refer to the Internet of the 1990s compared to the worldwide web of today. In addition, for purposes of coherence, this Article distinguishes between the consumption of online content, which can be thought of as “input” from the Internet, and the creation, publication, and communication of online content, which can be thought of as “output” to the Internet. Both have undergone significant change and, thus, have new and likely still developing roles in the modern online information ecosystem.

As a very basic matter, the last two decades have seen a significant evolution in the way that web services are delivered to consumers and a corresponding dramatic increase in the consumption of online content. The characteristics and capabilities of today’s most ubiquitous smartphones would have been virtually unthinkable in the 1990s, when which most mobile devices had only cellular phone functionalities and even those that were capable of connecting to the Internet could do so only through cables. The modern smartphone has wireless Internet capabilities, and more than two-thirds of Americans use these devices to follow breaking news, share media and/or information with others via the web, and stay up to date on activities and events in their communities. The volume of online content consumption has also grown by leaps and bounds: in 1997, just

---

69 Benkler, supra note 9, at 32–33.

70 It may be worth noting that there are no exact boundaries between “Web 1.0” and “Web 2.0”; indeed, even Tim O’Reilly, the tech-industry expert who popularized the term, acknowledges that there are no precise definitions for the terms and suggests that the two concepts are best understood by way of a cluster of characteristics. See O’Reilly, supra note 67. I adopt the terminology here only for the sake of simplicity and because while the boundaries may be hazy, the categories are, broadly speaking, descriptive of the two paradigms I discuss in this Part.


over one-third of Americans reported having a household computer and only eighteen percent reported accessing the Internet at home, as compared to about seventy-six percent with computers and seventy-one percent with Internet in 2011, according to the U.S. Census Bureau. The percentage of adults that use the Internet increased from fourteen percent in 1995 to nearly eighty percent in 2011, and those adults who use the Internet are reportedly partaking in an increasing range and volume of activities online.

Separate and apart from the input revolution, the ways in which Internet content output occurs have undergone a fundamental shift over the course of the last two decades. The paradigmatic online content models of the 1990s bore a reasonably close resemblance to the information-sharing models of traditional media: as with books, newspapers, radio, and television, the author and audience’s roles in the development and consumption of early online content were cleanly defined, and most “users” were merely passive readers. Crowdsourcing was virtually unheard of in the form in which we know it today, and webpages

---

75 Id. at 11 (“While internet adoption has been more or less stable over the past few years, there has been significant growth in the activities internet users engage in once they are online.”).
76 See David Croteau & William Hoynes, Media/Society: Industries, Images, and Audiences 297 (5th ed. 2014) (observing characteristics of traditional mass media, including (1) a one-to-many model of communication, (2) a known sender and an often anonymous or difficult-to-identify readership, (3) one-way transmission of information, and (4) defined roles for producers and receivers).
77 See, e.g., Sareh Aghaei et al., Evolution of the World Wide Web: From Web 1.0 to Web 4.0, 3 INT’L J. WEB & SEMANTIC TECH. 1, 2 (2012) (observing that Web 1.0 was generally “read-only . . . static and somewhat mono-directional”); Cormode & Krishnamurthy, supra note 67 (“[T]he essential difference between Web 1.0 and Web 2.0 is that content creators were few in Web 1.0 with the vast majority of users simply acting as consumers of content, while any participant can be a content creator in Web 2.0 and numerous technological aids have been created to maximize the potential for content creation.”); Karan Patel, Incremental Journey for World Wide Web, 3 INT’L J. ADVANCED RES. COMPUTER SCI. & SOFTWARE ENGINEERING 410 (2013) (observing that “the early web allowed us to search for information and read it,” and that there existed “very little in the way of user interaction or content contribution”); see also Benkler, supra note 9, at 153 (“The alternative of building some portions of our telecommunications and information production and exchange systems as commons was not understood in the mid-1990s, when the policy that resulted in this market structure for communications was developed.”); Dorota Piontek, New Media, Old Theories, 2 REVOLUTIONS 70, 71 (2014) (“As well as traditional media, Web 1.0 allows for static viewing of the content offered by the media.”).
were generally static pages hosted or run by third parties, which featured only one-way communication and had none of the interactive features that are generally associated with today’s worldwide web.\textsuperscript{79} The self-expression and production opportunities that did exist—for instance, email, discussion boards, and chat rooms—could be analogized to real-world or traditional media models of communication, and were unlikely to gain widespread readership due to the primitive nature of search engines,\textsuperscript{80} absence of social media,\textsuperscript{81} and relative lack of tools designed to facilitate content-sharing.\textsuperscript{82}

The Internet’s development over the last two decades has been nothing short of revolutionary. Today’s Internet is heavily interactive, if not user-driven,\textsuperscript{83} Web 2.0 users are said to be “as important as the content they upload and share with others.”\textsuperscript{84} Communications are multi-directional,\textsuperscript{85} breaking from the clean-cut distinction that prevailed in traditional media between author and audience and creating a less centralized, more democratic model of communication and information sharing.\textsuperscript{86} The critical shift is that from a publishing-based

\textsuperscript{79} See Aghaei et al., \textit{supra} note 77, at 2–3; Patel, \textit{supra} note 77, at 410; cf. O’Reilly & Battelle, \textit{supra} note 78, at 2 (describing the new features of the modern web).

\textsuperscript{80} See O’Reilly, \textit{supra} note 67 (comparing search capabilities over time).

\textsuperscript{81} See Cormode & Krishnamurthy, \textit{supra} note 67 (observing that social media platforms and functions are generally associated with Web 2.0).

\textsuperscript{82} O’Reilly, \textit{supra} note 67; Patel, \textit{supra} note 77, at 411 (“The main technologies and services of web 2.0 . . . included blogs, really simple syndication (RSS), wikis, mashups, tags, folksonomy, and tag clouds . . . .”).

\textsuperscript{83} See Croteau & Hoynes, \textit{supra} note 76, at 298; Cormode & Krishnamurthy, \textit{supra} note 67.

\textsuperscript{84} Patel, \textit{supra} note 77, at 411; see also Michele Hilmes, \textit{Only Connect: A Cultural History of Broadcasting in the United States} 418 (4th ed. 2014) (“Feeding these new devices were new desires: for enhanced participation and interactivity, for seamless cross-platform availability, for online spaces and places that you control, you shape, you build for yourself.”). The heavily user-centric zeitgeist of Web 2.0 famously prompted \textit{Time} to name “You” as the magazine’s 2006 Person of the Year. Lev Grossman, \textit{You—Yes, You—Are \textit{TIME}’s Person of the Year}, \textit{Time} (Dec. 25, 2006), http://content.time.com/time/printout/0,8816,1570810,00.html. In an essay accompanying the cover story, a writer observed that Andy Warhol’s famous prediction that everyone would one day be famous for fifteen minutes “has been replaced by a new prophecy: ‘On the Web, everyone is famous to 15 people.’ Appropriately enough, many people share authorship of that one.” Josh Tyrangiel, \textit{Andy Was Right}, \textit{Time} (Dec. 25, 2006), http://content.time.com/time/magazine/article/0,9171,1570780-1,00.html.

\textsuperscript{85} Croteau & Hoynes, \textit{supra} note 76, at 298.

\textsuperscript{86} Id.; see Benkler, \textit{supra} note 9, at 3 (observing that the information economy facilitated by today’s Internet “allows for an increasing role for nonmarket production in the information and cultural production sector, organized in a radically more decentralized pattern than was true of this sector in the twentieth century”).
model to a participation-driven framework, with the driving purpose of “harnessing collective intelligence.”

Two other points about this paradigm shift are particularly noteworthy. First, the sheer amount of information communicated via the Internet has increased exponentially over the course of the last two decades. Second, in keeping with the shift toward a more integrated, networked, and sharing-oriented information economy, syndication and aggregation have taken on increasingly important roles in the delivery of news and information on the modern worldwide web. Taken together, these developments create an information ecosystem in which individual voices would seem to be not only amplified but also repeated or multiplied. Professor Yochai Benkler has posited that this and other fundamental shifts in modern technology and communications have given rise to a “networked information economy,” which is characterized by an increase in “decentralized individual action—specifically, new and important cooperative and coordinate action carried out through radically distributed, nonmarket mechanisms that do

---

87 See O’Reilly, supra note 67; see also Hilmes, supra note 84, at 417–18; Aghaei et al., supra note 77, at 3. Today’s zeitgeist is perhaps most readily apparent in the proliferation of social media such as Facebook, Twitter, LinkedIn, and Instagram. See O’Reilly & Battelle, supra note 78, at 1 (“[P]owerful new platforms like YouTube, Facebook, and Twitter have demonstrated that same insight in new ways. Web 2.0 is all about harnessing collective intelligence.”). It is also readily demonstrated by other key features of today’s Internet such as digital interface more generally (e.g., wikis, blogs, and the ability to leave feedback via commentary), syndication, aggregation, and crowdsourcing. See Hilmes, supra note 84, at 417–20; Patel, supra note 77, at 411.

88 O’Reilly & Battelle, supra note 78, at 1.

89 See, e.g., Cisco, supra note 6, at 5 & tbl.1 (reporting on the explosion in the volume of Internet traffic between the 1990s and the present day).

90 See Charles Brown, Social Media, Aggregation and the Refashioning of Media Business Models, in HANDBOOK OF SOCIAL MEDIA MANAGEMENT 219, 220–23 (Mike Friedrichsen & Wolfgang Mühl-Benninghaus eds., 2013); see also Hilmes, supra note 84, at 418–20. Aggregation is considered a central feature of the modern news media, and as used in this journalistic context, the term refers to the (sometimes controversial) practice of curating news produced by others. See Bill Grueskin et al., COLUMBIA JOURNALISM SCH., TOW CTR. FOR DIG. JOURNALISM, THE STORY SO FAR: WHAT WE KNOW ABOUT THE BUSINESS OF DIGITAL JOURNALISM 83–91 (2011); Raymond Baldino, Content Aggregation: Spreading or Stealing the News?, 36 NEWS MEDIA & L. 21 (2012). Outside the news media context, “aggregation” may be used to refer to practices by any number of different sites, platforms, and software that involve pulling content from sources around the web, including RSS feeds, social media aggregators such as Hootsuite, apps such as Flipboard, and websites such as Rotten Tomatoes. See Fraser Sherman, How to Build an Aggregator Website, HOUS. CHRON.: SMALL BUS., http://smallbusiness.chron.com/build-aggregator-website-35778.html (last visited Mar. 31, 2016); see also Jill Duffy, 21 Great Apps and Tools for Social Media, PCMag (Mar. 13, 2012), http://www pcmag com/article2/0,2817,2401298,00.asp; Liam Lacey, The Studios Wake Up to the Power of Rotten Tomatoes, GLOBE & MAIL (Aug. 26, 2011), http://web.archive org/web/20110826142834/http://www.theglobeandmail.com/news/arts/movies/li am-lacey/the-studios-wake-up-to-the-power-of-rotten-tomatoes/article2142069/. Here, I use the term to describe both forms, as they have similar implications for purposes of this Article.
In short, the Internet revolution has created a dramatically different system of creation, communication, and consumption, which allows for more varied models of authorship and exponentially greater audience reach.

III. PROBLEMS WITH THE CURRENT LEGAL LANDSCAPE

In the face of considerable uncertainty as to the likely effect of regulating speech online, Congress—ostensibly driven by the desire to avoid compromising the enormous promise of the then-nascent Internet—made the decision to regulate conservatively. Thus, the court interpreted § 230 to preclude websites and service providers from being held liable for defamatory content posted by third parties outside of an extremely narrow subset of circumstances in which they had some active hand in the unlawful aspect of the actionable content. Courts that have addressed the issue have suggested that even inducing third-party users to post unlawful content is not certain to give rise to liability under the CDA. Moreover, websites and service providers are not required to investigate or remove actionable content after receiving complaints about it, though the statute will protect them if they choose to do so.

With the benefit of nearly two decades of case law under the CDA, it is now possible to reexamine the policy considerations underlying the statute and evaluate their continued validity in the modern Internet age. To do so, this Part first analyzes the currently prevailing judicial understanding of the policy objectives underlying § 230 in order to assess whether the provision has been correctly interpreted in the case law to date. It then considers whether, in

---

91 BENKLER, supra note 9, at 3.
92 47 U.S.C. § 230(b)(2) (2014); see also 141 CONG. REC. 22,045 (1995) (statement of Rep. Wyden) (“The Internet is the shining star of the information age, and Government censors must not be allowed to spoil its promise.”); id. at 16,014 (statement of Sen. Feingold) (“The use of computer networks holds tremendous potential for the expansion of public dialog and discourse . . . . It would be devastating to limit the potential of this medium by taking steps that could have the effect of silencing its users.”).
93 See sources cited supra note 46.
94 See Universal Commc’n Sys. v. Lycos, 478 F.3d 413, 421 (1st Cir. 2007) (leaving open the question of whether Lycos would be liable for actively inducing a third party to post actionable content). *But see* FTC v. Accusearch, Inc., 570 F.3d 1187, 1200 (10th Cir. 2009) (holding that defendant was liable for unlawful content when it had “affirmatively solicited” this content).
95 See, e.g., Ricci v. Teamsters Union Local 456, 781 F.3d 25 (2d Cir. 2015) (holding that GoDaddy could not be held liable for refusing to take down allegedly unlawful content posted on one of the websites it hosted); Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997) (holding that AOL was not obligated to take down potentially defamatory content, even after the plaintiff had complained and thereby put AOL on notice).
96 § 230(c)(2).
light of intervening developments in technology and our understanding of the Internet, these justifications continue to support § 230 in its current form. This Part concludes with a summary of certain independent problems with the current legal framework as it has been applied in a handful of recent cases. Ultimately, these observations show that § 230 must be updated to reflect the realities of the modern Internet and create more socially desirable policies and incentives.

A. Understanding the Policy Rationales Behind Section 230

As discussed in Section I.B, § 230 was enacted in order to (1) promote the development of the Internet by avoiding any potential deterrent effect on free speech, and (2) encourage websites and Internet service providers to self-regulate without fear of liability.\textsuperscript{97} These policy objectives, however, must be understood in the context of the CDA as a whole. While § 230 employs broad language in describing the provision’s statutory purpose,\textsuperscript{98} a closer examination of the legislative history strongly indicates that the first objective cited in connection with the scope of § 230—that is, to promote the development of the Internet and avoid chilling speech online—should instead be conceived of more narrowly.\textsuperscript{99}

The anti-indecency provisions set forth in other sections of the CDA were met with enormous skepticism in both the House and Senate. As introduced in the Senate, an early version of the bill made it a federal crime punishable by up to $100,000 in fines and two years’ imprisonment to send obscene or indecent material to minors, or to make this material available to minors, using a telecommunications device.\textsuperscript{100} The bill would have imposed the same penalties on individuals who knowingly permitted prohibited material to be communicated via telecommunications channels or platforms under the individuals’ control,\textsuperscript{101} and exempted only an extremely narrow class of service providers that did nothing but “provide access or connection” to the Internet and had no knowledge of the unlawful activity.\textsuperscript{102}

\textsuperscript{97} See supra notes 41–44 and accompanying text. As discussed supra Section I.B, the danger of “heckler’s vetoes” ostensibly served as another motivating factor; however, because this rationale appears to have been less prominent and relied upon less often by courts, I focus here primarily on the development and self-regulation rationales behind the passage of § 230.

\textsuperscript{98} See § 230(b).

\textsuperscript{99} See, e.g., 141 CONG. REC. 16,013–15 (1995) (statement of Sen. Feingold) (voicing fears about the potential chilling effects of the proposed legislation); see also infra notes 100–111 and accompanying text.

\textsuperscript{100} S. 652, 104th Cong., § 402 (1995).

\textsuperscript{101} Id.

\textsuperscript{102} Id. § 402(a). The cosponsors of the bill confirmed this narrow reading. See 141 CONG. REC. 16,025 (1995) (Sen. Exon).
Opponents of the bill primarily raised concerns about its constitutionality, but importantly, they also expressed major reservations based on the legislation’s potential implications for the growth and development of Internet technology and the web. Critics quickly pointed out that the bill would criminalize a vast range of constitutionally protected behavior and material, including literature, health information, and communications between adults that even peripherally touched on topics that could be considered indecent. Moreover, these critics argued that the bill’s sponsors fundamentally misunderstood the nature of the Internet, and that the legislation did not account for the reality that it is all but impossible to truly ascertain audience members’ identities online. Under the proposed statutory scheme, they argued, liability could perhaps be imposed on any individual who posted indecent material on an online forum or bulletin board, since knowledge could be imputed to that individual that a minor might log onto the site and view the material. It was in response to this legislative proposal—and apparently not, as some courts have suggested—to the specter of tort and criminal liability as a general matter—that legislators sounded the alarm about the need to avoid chilling effects on free speech and ultimately added § 230 to the bill.


104 See, e.g., id. at 22,045 (statement of Rep. Wyden) (“Mr. Chairman and colleagues, the Internet is the shining star of the information age, and Government censors must not be allowed to spoil its promise.”); id. at 16,013 (statement of Sen. Feingold) (“I am concerned that this legislation will have a chilling effect . . . potentially slowing the rapid technological advances that are being made in this new technology.”).

105 See id. at 16,020 (statement of Sen. Leahy) (observing that the statute would prohibit, inter alia, transmission of D.H. Lawrence, Lady Chatterly’s Lover (1928) to a minor); id. at 16,014 (statement of Sen. Feingold) (noting that the statute might criminalize discussions in online support groups about sexual or domestic abuse, or the transmission of information about preventing STIs and AIDS).


108 See supra notes 36–45 and accompanying text.

109 141 Cong. Rec. 16,014 (1995) (statement of Sen. Feingold) (“This threat of criminal sanctions could have a dramatic chilling effect on free speech on interactive telecommunications systems, and in particular, these newsgroups and bulletin boards accessed through the Internet. Quite simply, adults will have to watch what they say on these forums.”); id. at 16,020 (statement of Sen. Leahy) (expressing the same concern); id. at 22,046 (statement of Rep. Goodlatte) (supporting a version of the bill that contained § 230 over a version that did not, reasoning that the version with section 230 “doesn’t violate free speech or the right of adults to communicate with each other”). Nowhere in any of the hearings on § 230 did the legislators explicitly refer to tort liability, though they did refer to the Supreme Court of New York’s decision in Stratton Oakmont, Inc. v.
The CDA initially introduced a danger of liability in connection with an extremely broad range of online activity, including anti-indecency clauses. Considering these legitimate threats to free speech on the Internet, § 230 immunity is defensible as a matter of policy when viewed in context of the CDA in its original form. However, this policy justification faded away when the Supreme Court invalidated the most constitutionally problematic aspects of the statute. Thus, the statutory provision makes very little sense as applied as a bar against modern tort suits: it was intended not to foreclose civil liability under the common law of tort, but to prevent the statute’s harsh prohibitions on certain kinds of content from inhibiting the development of technology. While the pro-self-regulation rationale that motivated § 230 retains some validity, the courts should understand the provision more narrowly, as just one part of the legal landscape following the enactment of the CDA—a significantly different regime from the one we know today—in order to reconcile the provision with its legislative history.

B. Reexamining the Policy Rationales Behind Section 230

Even if the prevailing justifications for § 230’s creation are correct, the provision still merits new consideration because today’s Internet is different from the Internet of 1996. When the Fourth Circuit first considered these policy rationales in an early (and important) § 230 case, Zeran v. America Online, Inc., a plausible argument existed that a laissez-faire approach to online content regulation would support the web’s revolutionary potential. Whatever the original

---


---

110 141 CONG. REC. 16,013–15 (1995) (statement of Sen. Feingold); Cannon, supra note 31, at 75–88. This logic is implicit in the Supreme Court’s 1997 opinion striking down the anti-indecency provisions. See Reno v. ACLU, 521 U.S. 844, 872 (1997) (“The severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images. As a practical matter, this increased deterrent effect, coupled with the ‘risk of discriminatory enforcement’ of vague regulations, poses greater First Amendment concerns than those implicated by [civil regulations].” (citations omitted)).

111 See Reno, 521 U.S. 844.

112 See supra Part II.

113 129 F.3d 327 (4th Cir. 1997).

114 Recall that at the time, the volume of Internet traffic was a tiny fraction of what it is today, see Cisco, supra note 7, at 5 & tbl.1, and that there were only an estimated forty million users around the globe, see Zeran, 129 F.3d at 334 (citing Reno, 521 U.S. at 850). In contrast, virtually all of today’s telecommunications are transmitted online, and the number of Internet users worldwide has skyrocketed to more than three billion. See INT’L TELECOMM’N UNION, TELECOMM’N DEV. BUREAU, ICT DATA & STATISTICS DIV., ICT FACTS AND FIGURES: THE WORLD IN 2015, at 1 (2015), http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.
purpose of § 230, it is clear that the Internet no longer requires such special legal protections in order to grow and flourish.\footnote{115}{Cf. 17 U.S.C. § 512 (2014) (regulating Internet service providers in order to police copyright infringement online).}

As the web has grown in size and social importance, the body of information about the Internet and how it operates has become increasingly robust. Experts in law and policy are now better able to understand the Internet and evaluate the laws that govern it in light of the original policy considerations. In this vein, Professor Lawrence Lessig has argued that the Internet is inherently more speech-protective than Congress seemed to suppose, simply by virtue of its basic design:

[O]n top of this list of protectors of speech in cyberspace is (once again) architecture. Relative anonymity, decentralized distribution, multiple points of access, no necessary tie to geography, no simple system to identify content, tools of encryption—all these features and consequences of the Internet protocol make it difficult to control speech in cyberspace. The architecture of cyberspace is the real protector of speech there; it is the real “First Amendment in cyberspace,” and this First Amendment is no local ordinance.\footnote{116}{LAWRENCE LESSIG, CODE 2.0, at 236 (2d ed. 2006).}

Professor Lessig and other scholars thus have noted that the institutional structure of the Internet itself goes a long way toward effectuating the sorts of policy goals that motivated Congress to enact § 230.\footnote{117}{Id.; see also, e.g., Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 STAN. L. REV. 1373, 1437–38 (2000) (acknowledging the fundamental role that the institutional design of online technology plays in protecting data privacy); Neal Kumar Katyal, Digital Architecture as Crime Control, 112 YALE L.J. 2261, 2283–86 (2003) (arguing, drawing upon Lessig’s work, that the government should regulate code in order to most effectively control crime in cyberspace).} This critical point—that is, the idea that institutional design, not direct regulation, supplies the primary constraints on private behavior online—did not emerge until after the CDA had been enacted.\footnote{118}{See Katyal, supra note 117, at 2261 (noting Professor Lessig’s “path-breaking scholarship isolating architecture as a constraint on behavior online,” which began in 1999 (citing LAWRENCE LESSIG, CODE 4–14 (1999))).}

Thus, the two decades since the CDA became law have yielded critical wisdom about regulation and the institutional realities of the Internet.

Today’s most influential websites reach beyond classic content models to include social media and dating websites, search engines, user-driven advertising platforms, file-sharing databases, user-generated news sites, and aggregators of...
other content drawn from around the web.\footnote{See, e.g., \textit{The Top 500 Sites on the Web}, ALEXA, http://www.alexa.com/topsites (last visited Apr. 1, 2016); see also, e.g., Eric Griffith, \textit{Top 100 Sites of 2014}, PC MAG (Jan. 9, 2015), http://www.pcmag.com/article2/0,2817,2474728,00.asp. For more information on this diversification in content models, and the evolution of the Internet more generally, see supra Section II.B.} Under § 230, however, these websites and service providers face no potential liability costs for defamatory content posted by third parties, even if they republish the material recklessly, edit it to make it more sensational, or refuse to remove it after being put on notice.\footnote{47 U.S.C. § 230(c)(1) (2014); see also supra note 95 and accompanying text.} There is little reason to believe that this scheme incentivizes websites and service providers to self-regulate given that there are no readily apparent prospective benefits to doing so.

Moreover, reevaluating § 230 is critical because such websites, in fact, stand to gain financially from unregulated speech conduct. Online content publication costs are extraordinarily low compared to the expenses associated with publishing via more traditional media such as print, television, and radio.\footnote{See Lessig, supra note 116, at 245–49 (observing that the lower costs associated with supplying objectionable content online will increase the demand for this content).} Creators and publishers of web content thus face fewer barriers to entry than do traditional media publishers, and can also communicate a greater volume of content at a lower cost.\footnote{\textit{Id.}} In a world in which traffic drives revenue,\footnote{See, e.g., \textit{Rick Edmons et al., Poynter Inst. & Pew Research Ctr., The State of the News Media 2013: An Annual Report on American Journalism} (2013); Kenneth Olmstead & Kristine Lu, \textit{Digital News—Revenue: Fact Sheet}, PEW RES. CTR. (Apr. 29, 2015), http://www.journalism.org/2015/04/29/digital-news-revenue-fact-sheet/; see also PricewaterhouseCoopers LLP & Interactive Advert. Bureau, IAB Internet Advertising Revenue Report: 2014 Full Year Results (2015); Felix Richter, Facebook’s Growth is Entirely Fueled by Mobile Ads, STATISTA (Nov. 30, 2015), http://www.statista.com/chart/2496/facebook-revenue-by-segment/.} this means that websites and service providers are incentivized to republish or let stand content that seems likely to attract attention and generate page views, regardless of whether or not the material is defamatory.

Thus, a defamatory blog post that could become “clickbait”\footnote{See James Hamblin, \textit{It’s Everywhere, the Clickbait}, ATLANTIC (Nov. 11, 2014), http://www.theatlantic.com/entertainment/archive/2014/11/clickbait-what-is/382545/ (discussing the concept of clickbait).} would be extremely attractive to a publisher of web content; and that publisher would have every reason to repost the material and publicize it prominently on the website’s main page, perhaps after adding search engine optimization to help draw additional traffic. In this respect, § 230 suffers a clear shortcoming in that it contributes to a set of legal and financial circumstances in which publishers and aggre-
gators of web content are, if anything, financially incentivized to republish—and, thereby, to effectively amplify—defamatory material, ultimately increasing the audience that the material is likely to reach. Thus, while the CDA can certainly be, and indeed has been, applied to the modern panoply of content models in the form in which it was originally written, the evolution of the Internet has rendered the statutory scheme outdated. The CDA ought to be revised to reflect these developments and establish more normatively desirable incentives for today’s websites and Internet service providers.

C. Examining Problematic Applications of Section 230

Section 230 has certainly been applied to immunize websites and Internet service providers in “easy” cases in which it is clear that practical and policy considerations marshal in favor of granting immunity. For instance, courts have held that search engines are not liable for allegedly defamatory impressions created by search results pages, and have maintained that websites that merely provide open forums for discussion and have no possible knowledge of allegedly actionable content posted by third parties are entitled to immunity under § 230. It has also been applied, however, in ways that lead to troubling or nonsensical outcomes due to the breadth of the immunity conferred by § 230. The problems illustrated by these cases, together with the diminished force of the policy ration-

---


127 See, e.g., O’Kroley, 2014 WL 2881526, at *1–2 (holding that Google was not liable for an allegedly defamatory impression created by its search results because “the automated editorial acts of Google in publishing the information which was the search result did not make Google an information content provider”).

128 See Klayman, 753 F.3d at 1358 (“[A] website does not create or develop content when it merely provides a neutral means by which third parties can post information of their own independent choosing online.”); Chi. Lawyers’ Comm. for Civ. Rights Under Law v. Craigslist, Inc., 519 F.3d 666, 672 (7th Cir. 2008) (“[Plaintiff] cannot sue the messenger just because the message reveals a third party’s plan to engage in unlawful discrimination.”); Universal Commc’n Sys. v. Lycos, 478 F.3d 413, 420 (1st Cir. 2007) (observing that there was “not even a colorable argument that any misinformation was prompted by Lycos’s registration process or its link structure”).
ales underlying § 230, strongly suggest that the statutory provision should be amended in keeping with the evolution of the modern digital age.

1. Troubling Outcomes

Section 230 has been applied in some cases, particularly in private actions arising out of alleged child-sex exploitation, in ways that lead to troubling and arguably suboptimal outcomes. Specifically, courts have held that § 230 immunizes interactive computer service providers against criminal liability when third parties transmit unlawful content, including child pornography. Even when the governing federal criminal statutory scheme provides for a private right of action, even if the website or service provider clearly knew or had reason to know that its platform was hosting this objectionable material, and even if the website or service provider ostensibly profited from the posting of the illegal material, such websites and service providers have been held to be entitled to § 230 immunity.

In one recent example, Doe v. Backpage.com, LLC, plaintiffs were underage girls who allegedly had been pimped out using ads on Backpage.com.129 In claiming that § 230 did not protect Backpage.com, plaintiffs pointed to the language in § 230(e)(1) stating that the statutory provisions would not immunize interactive computer service users and providers against federal criminal law.130 The court rejected this argument on the ground that although the CDA expressly did not provide immunity from criminal liability, it did immunize defendants against civil suits brought by private plaintiffs.131 According to the court, it made no difference that the federal anti-sex-trafficking statute expressly provided victims of sex trafficking with a private right to bring civil actions against “whoever knowingly benefits, financially or by receiving anything of value from participation in a venture which that person knew or should have known has engaged in an act in violation of this chapter.”132 A private, civil suit did not constitute enforcement of the criminal statute, the court reasoned, and thus the defendant website’s claim to immunity under § 230 succeeded.133

In another recent case, the U.S. District Court for the Eastern District of Texas arrived at an even more troubling conclusion when it refused to impose civil liability on Yahoo! for child pornography that had been exchanged in one of

---

130 Id. at 158–60.
131 Id.
132 Id. at 158 (quoting 18 U.S.C. § 1595 (2014)) (internal quotation marks omitted).
133 Id. at 158–60.
Yahoo!’s e-groups.\textsuperscript{134} The moderator of the e-group had been sentenced to prison for the same conduct that gave rise to the civil action, and plaintiffs claimed that both Yahoo! and the moderator had known about the illegal content being communicated through the group.\textsuperscript{135} In rejecting the plaintiffs’ claim to relief, the court stated, “Section 230 does not, as Plaintiffs propose, provide that an intentional violation of criminal law should be an exception to the immunity from civil liability given to internet service providers.”\textsuperscript{136} It also ruled that the fact that Yahoo! in fact earned money from the e-group was irrelevant: “Plaintiffs make much of the allegation that Yahoo! profited from advertising on the ‘Candyman’ e-group. However, Plaintiffs have not shown that Congress intended the question of immunity to turn on how the internet service provider earns its revenue, whether by subscription fees or by advertising.”\textsuperscript{137}

2. Nonsensical Outcomes

In another subset of cases, § 230 has led to results that seem to make little practical sense, particularly in light of the power and prevalence of today’s Internet. For instance, in AdvanFort Co. v. Maritime Executive, LLC, the U.S. District Court for the Eastern District of Virginia considered a claim against defendant The Maritime Executive (“TME”), a maritime journal that had allegedly published defamatory material about the plaintiff.\textsuperscript{138} The court ultimately held that the plaintiff’s claim could proceed—and that the defendant’s claim to complete immunity under the CDA failed—because while TME would have been entitled to this immunity the newsletter containing the allegedly defamatory content only been published online, there was some evidence indicating that the newsletter was in fact circulated in print, as well.\textsuperscript{139} If the newsletter had indeed been published in printed format, then the CDA would not apply and the defendant could potentially be held liable as a publisher of the material under the state law of defamation.\textsuperscript{140}

Perversely, a defendant can be liable under § 230 for providing print copies of a newsletter containing defamatory material but is not liable if the same content was only printed online. This standard is paradoxical—printed papers ostensibly have a rather limited reach in terms of circulation but digital content is

\begin{itemize}
\item[135] Id. at *2–7.
\item[136] Id. at *9.
\item[137] Id. at *9–10.
\item[139] Id.
\item[140] Id.
\end{itemize}
available to a readership that literally spans across the globe. Furthermore, this
rule is at odds with many of the doctrinal underpinnings of the common law of
defamation, which provided states with the leeway to strike a balance between
reputational interests and free speech values. Ignoring this calculated balance
by individual states, the broad application of § 230 provides a preemptive blanket
grant of immunity at the federal level and raises implications about the basic
principles of federalism. As AdvanFort Co. demonstrates, this assertion of feder-
al-level immunity allows for widespread speech that states would deem action-
able were the speech to appear over alternative, less permanent, traditional me-
dia formats, such as the radio, on TV, or in print. The statute undercut states’
offline attempts to protect reputational interests by providing such broad immuni-
ty online.

IV. REFORMS

As the preceding Part describes, the two main rationales that courts have
drawn upon when addressing § 230 no longer apply in full force. Furthermore,

---

141 The common law of defamation reflected the principle that some types of defamatory
communications were more harmful or dangerous than others. See Restatement (Second) of the
Law of Torts §§ 569, 570 (Am. Law Inst. 1977); see also, e.g., Varian Med. Sys. v. Delfino, 6
Cal. Rptr. 3d 325, 340–43 (2003) (observing that the distinction between libel and slander matters
due to the implications for the availability of special damages). The size of the audience to which
the material was being disseminated and the permanence (or “persistence”) of the defamation were
considered relevant to the determination as to which category a particular communication be-
longed. Restatement (Second) of the Law of Torts § 568(3). These considerations, as applied
to the Internet, would seem to indicate that defamatory material published online should be consid-
ered more dangerous rather than less, and thus more readily give rise to liability.

142 See generally Melville B. Nimmer, The Right to Speak from Times to Time: First
Amendment Theory Applied to Libel and Misapplied to Privacy, 56 Calif. L. Rev. 935 (1968);

143 See, e.g., The SAGE GUIDE TO KEY ISSUES IN MASS MEDIA ETHICS AND LAW 190 (William
A. Babcock & William H. Freivogel eds., 2015) (“While material on the Internet may seem
less permanent than printed materials, since it can constantly be edited or even ‘deleted,’ the truth is
that postings online and in emails can reappear after they appear to have been deleted.”); Jeffrey
are only beginning to understand the costs of an age in which so much of what we say, and of what
others say about us, goes into our permanent—and public—digital files.”).

144 See, e.g., AdvanFort Co., 2015 U.S. Dist. LEXIS 99208, at *25–30; see also Jae Hong
Lee, Batzel v. Smith & Barrett v. Rosenthal: Defamation Liability for Third-Party Content on the
Internet, 19 Berkeley Tech. L.J. 469, 485 (2004) (observing the different standards of liability
imposed for print and online defamation); Tracie Powell, Online Publishers Still Aren’t Usually
Liable for User-Generated Content, Colum. Journalism Rev. (June 19, 2014) (observing that the
Sixth Circuit’s ruling in Jones v. Dirty World Entertainment Recordings LLC, 755 F.3d 398 (6th
Cir. 2014), “leaves in place, for now, immunity that websites enjoy when it comes to publishing
third-party content—like online comments on news sites—as long as the website does not add any
unlawful material to that content,” but that this immunity “does not extend to letters to the editor in
print publications, paper’s version of user-generated content”).
the statute has repeatedly been applied in ways that yield incongruous or unfair results. Therefore, the policy considerations behind § 230 marshal in favor of narrowing the scope of the immunity conferred on websites and Internet service providers. This Part presents three potential reforms, each of which could be deployed to more effectively strike an appropriate balance between the interests at stake in the online defamation context and help avoid the problematic outcomes associated with § 230 in its current form.

A. The United Kingdom’s Approach

The first potential reform would establish a liability regime akin to the one currently in force in the United Kingdom. The law of online defamation in the United Kingdom features, *inter alia*, a “notice-and-takedown” scheme designed to deter websites from continuing to make available defamatory content created by third parties.\(^{145}\) The United Kingdom’s Defamation Act of 2013 establishes that an operator of a website that features user-generated content can defend against a defamation action by demonstrating that a user, rather than the operator, was responsible for posting the defamatory material.\(^{146}\) However, the statute also provides that a plaintiff can overcome this defense—and the website operator can be held liable—if the plaintiff can show that the user responsible for the content cannot be identified and that the website operator did not respond to the plaintiff’s complaint, notification, or takedown request in a timely fashion.\(^{147}\) Thus, this statute imposes a very real threat of liability based on defamatory third-party content.\(^{148}\)

This standard is preferable to the scheme set forth in the CDA for three primary reasons. First, the rule would help ensure that plaintiffs injured by defamation are compensated, either by the actual injurer or by the website or service provider. Second, because website operators will only be held liable if the third-party user who posted the actionable material remains unidentified, the scheme as a default matter imposes liability upon the party truly responsible for the defamation. Finally, the notice-and-takedown system incentivizes website owners and Internet service providers (“ISPs”) to respond promptly to takedown requests.\(^{149}\)

\(^{145}\) Defamation Act 2013 c. 26, § 5(2) (Eng.).

\(^{146}\) See id.

\(^{147}\) Id. § 5(3).

\(^{148}\) See, e.g., Tamiz v. Google Inc. [2013] EWCA (Civ) 68 (appeal taken from Eng.) (holding that the defense was overcome and that defendant Google could be held liable for defamation, based on a five-week delay in Google’s response to plaintiff’s takedown request).

\(^{149}\) A recent study found that the United Kingdom’s approach has been highly effective at removing defamatory content from the Internet—or at least removing it to the extent possible, so that it is unavailable to the public at large. See Tyler Moore & Richard Clayton, *The Impact of Incentives on Notice and Take-Down* (“Where a court action is unlikely, the practical effect of the
Because the swift removal of defamatory content can help limit the audience that ultimately views the material—and given the fact that these interactive computer services providers are in the best position to take down the problematic content—this system would place the burden of mitigation with the entities that are best situated to take effective steps to this end.  

This is not to say that there are no potential objections to the United Kingdom’s scheme. There are legitimate questions as to whether this might result in the “heckler’s veto,” wherein citizens would be able to effectively censor websites simply by claiming that hosted content is defamatory. Any risk of a true “veto,” however, could potentially be mitigated with a corollary to the takedown requirement that would require websites and service providers to replace content that was temporarily removed in response to defamation claims once those websites determined that the content was not defamatory. Under this scheme, the website’s duty is not truly one of removal, but rather one of investigation. At least one other statutory scheme in the United States establishes a similar corollary rules structure—albeit without an identification option that would allow the publisher to escape liability. Specifically, the Digital Millennium Copyright Act (“DMCA”) establishes a similar liability rule with respect to online content that unlawfully infringes upon copyrights in violation of federal law.  

The other major potential objection to this proposal would advance a constitutional argument. The Supreme Court has recognized that, in some circumstances, there exists a right to anonymous speech. As an initial matter, anonymity in the context of online commentary clearly differs somewhat from the political contexts in which the Court has vindicated these free speech rights.  

different US and UK regimes is that when defamatory content is published on a UK web site it will be fairly promptly removed by the ISP. When it is republished on a US site, it then remains available for a considerable time. )., in MANAGING INFORMATION RISK AND THE ECONOMICS OF SECURITY 199 (Eric M. Johnson ed., 2009). The study authors also found, however, that this appears to have deterred website hosts from operating in England, which indicates that the anti-defamation gains from this approach might come at the expense of commercial benefit. Id. at 221.  

Danielle Keats Citron & Helen Norton, Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age, 91 B.U. L. REV. 1435, 1439 (2011) (observing the fact that intermediaries have significant control over the material that appears on their sites).  

See supra note 44 and accompanying text.  

See 17 U.S.C. § 512(c), (g) (2014).  

See id.  

See, e.g., McIntyre v. Ohio Elections Comm’n, 514 U.S. 334, 342 (1995) (“[A]n author’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.”); Talley v. California, 362 U.S. 60, 69 (1960) (“Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind.”).  

See McIntyre, 514 U.S. at 342–43; Talley, 362 U.S. at 69.
Nevertheless, there may be a legitimate question as to whether a statutory scheme with an identification provision of this nature comports with First Amendment doctrine.\footnote{156 See Doe v. Harris, 772 F.3d 563 (9th Cir. 2014) (affirming a district court’s decision to enjoin enforcement of California’s Proposition 35, which required convicted sex offenders to file a list of their Internet aliases with the government, on the ground that the law’s restrictions on anonymous speech rendered it constitutionally suspect), aff’g No. C12–5713-THE, 2013 WL 144048 (N.D. Cal. Jan. 11, 2013). See generally Sophia Qasir, Anonymity in Cyberspace: Judicial and Legislative Regulations, 81 FORDHAM L. REV. 3651 (2013); Jason M. Shepard & Genelle Belmas, Anonymity, Disclosure and First Amendment Balancing in the Internet Era: Developments in Libel, Copyright, and Election Speech, 15 YALE J.L. & TECH. 92 (2012); Matt Peckham, The New York Bill that Would Ban Anonymous Online Speech, TIME (May 24, 2012), http://techland.time.com/2012/05/24/the-new-york-bill-that-would-ban-anonymous-online-speech/.

\footnote{157 See Shepard & Belmas, supra note 156, at 133 (observing the complications that the Internet has introduced into this doctrinal area).}

\footnote{158 See, e.g., McIntyre, 514 U.S. at 342–43.}

\footnote{159 See, e.g., Citizens United v. FEC, 558 U.S. 310, 370 (2010) (rebuffing a challenge by Citizens United to a statutory requirement that political donors’ identities be disclosed when Citizens United had “identified no instance of harassment or retaliation”); Doe v. Reed, 561 U.S. 186, 200 (2010) (“[T] hose resisting disclosure can prevail under the First Amendment if they can show ‘a reasonable probability that the compelled disclosure [of personal information] will subject them to threats, harassment, or reprisals from either Government officials or private parties.’” (alteration in original) (quoting Buckley v. Valeo, 424 U.S. 1, 74 (1976))); Talley, 362 U.S. at 64; see also Qasir, supra note 156, at 3670 (observing the potentially different interests at work in political speech and anonymous online speech). But see Jonathan Turley, Registering Publius: The Supreme Court and the Right to Anonymity, 2001 CATO SUP. CT. REV. 57, 77 (discussing the importance of anonymous online speech).

\footnote{160 Cf. 17 U.S.C. §512(c) (2014) (regulating copyright-infringing speech by regulating intermediaries); Bradley A. Areheart, Regulating Cyberbullies Through Notice-Based Liability, 117 YALE L.J. POCKET PART 41 (2007), http://yalelawjournal.org/forum/regulating-cyberbullies-through-notice-based-liability (arguing that a system of notice-based liability for intermediaries would be constitutional in the context of libel law, provided that the law was sufficiently narrowly tailored); Jack M. Balkin, Old-School/New-School Speech Regulation, 127 HARV. L. REV. 2296, 2306–14 (2014) (discussing the forms of intermediary liability that have come to serve as partial replacements for traditional, direct regulations of speech).}
bility. When these websites and service providers are not governmental actors, they are private intermediaries that can independently choose to require users to register, and the reform would allow them to retain the discretion to choose otherwise. Under these circumstances, an attack on the proposed reform based on the right to anonymous speech ought to carry substantially less persuasive force.


The second potential avenue for reform would restore a fault-based liability framework for ISPs and websites through an amendment to § 230. This change would more closely reflect the scheme that governed at common law in that blanket immunity would not be available to publishers as a class. Internet and non-Internet publishers alike would be subjected to a single framework with respect to the entities that could be held liable, which ostensibly would help eliminate nonsensical case outcomes such as that in AdvanFort Co.

Under this amended statutory scheme, a website would be subject to the common-law standards of distributor or publisher liability, depending on the degree of review or editorial control that it actually exercised over the defamatory material. The news website that aggregates and curates content from around the web would be held to the liability standard that typically governs publishers,

---

161 It is possible, of course, for government entities to be interactive computer service providers for purposes of the CDA, given the fact that they may be responsible for the content of websites in the .gov domain.

162 Private-sector websites and service providers generally will not be considered government actors, and thus will not be subject to First Amendment suits. See, e.g., Green v. Am. Online, 318 F.3d 465, 472 (3d Cir. 2003) (holding that AOL could not be considered a state actor); see also Citron & Norton, supra note 150, at 1453. Moreover, these websites and service providers will be subject to the protection of the CDA’s Good Samaritan provision. See 47 U.S.C. § 230(c)(2) (2014).

163 For discussions of the propriety of regulating online speech through intermediaries such as websites and service providers, see Areheart, supra note 160; Balkin, supra note 160; Sophie Stalla-Bourdillon, Making Intermediary Internet Service Providers Participate in the Regulatory Process Through Tort Law: A Comparative Analysis, 23 INT’L REV. L. COMPUTERS & TECH. 153 (2009); Christopher S. Yoo, Free Speech and the Myth of the Internet as an Unintermediated Experience, 78 GEO. WASH. L. REV. 697 (2010).

164 See RESTATEMENT (SECOND) OF TORTS § 577 (AM. LAW INST. 1977); supra Section I.A.


166 Cf. RESTATEMENT (SECOND) OF TORTS § 578 (AM. LAW INST. 1977) (providing that those who republish or repeat defamatory content are subject to the same liability as original publishers of that content, unless they “only deliver or transmit defamation published by a third person”).
consistent with its ability to edit the objectionable content prior to publication.\footnote{167} A platform such as Facebook, however—in which the third-party users, not the company’s employees, are responsible for the initial publication of actionable material to the site—would likely be subject to the lesser standard of distributor liability.\footnote{168} The news website would be liable for the content as an initial matter because, by virtue of its editorial control over the material, it would have known or had reason to have known about the defamatory nature of the content prior to publication; on the other hand, Facebook could be held liable only if it failed to take action upon receiving notice of questionable content.\footnote{169}

The precise framing of the fault-based liability standard would have to comport with the constitutional requirements that the Supreme Court recognized in cases such as \textit{New York Times Co. v. Sullivan},\footnote{170} \textit{Curtis Publishing Co. v. Butts},\footnote{171} and \textit{Gertz v. Robert Welch, Inc.}\footnote{172} Rather than various standards imposing different outer limits based on the defamed individual’s status as a public official, public figure, or private figure, however—à la the common-law framework as complicated by this constitutional overlay\footnote{173}—a single rule, namely the \textit{New York Times} “actual malice” rule, should govern in all online defamation cases.\footnote{174} Under this system, courts could still consider whether the allegedly defamatory

\footnote{167} \textit{Id.} § 577(2).

\footnote{168} \textit{Id.} § 578. In this context, Facebook ostensibly would be considered a “deliverer” or “transmitter” of defamatory content rather than a repeater or republisher, since the site would merely provide the platform for the transmission of the content. The site does not moderate its users’ pages, does not review content prior to publication, and does not, for instance, repost or aggregate the material at other locations online. See Emma Barnett & Iain Hollingshead, \textit{The Dark Side of Facebook}, \textit{TELEGRAPH} (Mar. 2, 2012), http://www.telegraph.co.uk/technology/facebook/9118778/The-dark-side-of-Facebook.html (describing Facebook’s content moderation process, which begins only when content is reported by a user). For a description and discussion of a contrasting moderation policy whereby all posted content is reviewed at the time of publication—which might trigger the more demanding standard of publisher liability—see Adrian Chen, \textit{The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed}, \textit{WIRED} (Oct. 23, 2014), http://www.wired.com/2014/10/content-moderation/ (discussing the “active moderation” system deployed by mobile startup Whisper).

\footnote{169} \textit{See supra} Section I.A.

\footnote{170} 376 U.S. 254 (1964).

\footnote{171} 388 U.S. 130 (1967) (plurality opinion).

\footnote{172} 418 U.S. 323 (1974).


\footnote{174} The Supreme Court has held that content that defames public officials cannot give rise to defamation liability unless the speaker or publisher of that content acted with actual malice. \textit{See Sullivan}, 376 U.S. at 279–80. Conversely, content that defames private individuals can constitutionally give rise to liability so long as the speaker or publisher was at least negligent. \textit{See Gertz}, 418 U.S. at 347. Thus, to comply with the First Amendment, a single standard would have to be consistent with the more demanding \textit{Sullivan} rule.
speech is a matter of public concern, but they would not need to look to the plaintiff’s status in order to determine whether the speech is unlawful or constitutionally protected.

Numerous practical considerations support the elimination of the public/private-figure dichotomy. In an era of social media, viral videos, and global publicity with a few quick keystrokes, it has become increasingly difficult to draw the line between public and private figures. This simplified legal framework would be clearer and perhaps more administrable, since the public/private figure determination would be removed from the equation entirely, and the unitary standard also might help reduce potential confusion among regulated actors.

Perhaps more importantly, the doctrinal development of the distinctions between public officials, public figures, and private figures provides at least some support for the use of the Sullivan standard in online defamation cases. In extending the actual malice standard to cases involving public figures, the Su-

\begin{footnotesize}\begin{enumerate}
\item[175] Cf. Obsidian Fin. Grp. v. Cox, 740 F.3d 1284, 1287 (9th Cir. 2014) (“We hold that liability for a defamatory blog post involving a matter of public concern cannot be imposed without proof of fault and actual damages.”); see also id. at 1291 (observing that the Supreme Court had never considered the applicability of the Gertz rule in cases involving allegedly defamatory statements not on matters of public concern).
\item[176] See, e.g., Jeff Kosseff, Private or Public? Eliminating the Gertz Defamation Test, 2011 J.L. TECH. & POL’Y 249, 250–51 (“Massive technological and economic changes in the media over the past three decades have rendered the Gertz public/private distinction unworkable and unfair.”); Ashley Messenger & Kevin Delaney, In the Future, Will We All Be Limited-Purpose Public Figures?, 30 COMM. LAW., Mar. 2014, at 4 (examining the limited-purpose public figure doctrine in the context of social media). Indeed, there has been much discussion about the ways in which the Internet age has transformed the way that society thinks about the public and private spheres. See John B. Thompson, Shifting Boundaries of Public and Private Life, THEORY CULTURE & SOC’Y, July 2011, at 49; Brad Stone, Our Paradoxical Attitudes Toward Privacy, N.Y. TIMES: BITS (July 2, 2008, 3:56 PM), http://bits.blogs.nytimes.com/2008/07/02/our-paradoxical-attitudes-towards-privacy/; see also Amanda Hess, Is All of Twitter Fair Game for Journalists?, SLATE (Mar. 19, 2014, 4:42 PM), http://www.slate.com/articles/technology/technology/2014/03/twitter_journalism_private_lives_public_speech_how_reporters_can_ethically.html (describing this issue as it arises among journalists today).
\item[177] The public/private figure dichotomy is an important one for journalists, for example, who want to know the limitations on the material they can cover in their reporting. See, e.g., REPORTERS COMM. FOR FREEDOM OF THE PRESS, THE FIRST AMENDMENT HANDBOOK 5–6, 10 (7th ed. 2011) (advising reporters on their First Amendment rights with respect to defamation law); Nisha Chittal, How to Decide What Can Be Published, What’s Private on Twitter and Facebook, POYNTER (Mar. 29, 2012), http://www.poynter.org/news/mediawire/167704/how-to-decide-what-can-be-published-whats-private-on-twitter-and-facebook/ (“As more journalists rely on social media to find ideas and sources, there is increasing confusion about what’s acceptable and what isn’t when it comes to using material not originally intended for publication.”); Defamation, DIG. MEDIA L. PROJECT, http://www.dmlp.org/legal-guide/defamation (last updated Aug. 12, 2008) (providing guidance to the media on modern defamation law).
\end{enumerate}\end{footnotesize}
The Supreme Court seemed to rely on two primary justifications: (1) both public officials and public figures have deliberately and unmistakably assumed the risk of negative publicity through their voluntary actions, and (2) both also have access to channels that will allow them to meaningfully reply to alleged defamation. The former (assumption of risk) rationale may not support this proposed doctrinal extension, but the latter (access to reply channels) very well could. Anyone with Internet access has the continuous power to reach a global audience, and the Supreme Court has not held that the audience composition and likely audience size need to be similar for both the defamatory content and the rebuttal. Moreover, the “assumption of risk” prong of this inquiry might matter less in the online context given the Internet’s—especially social media’s—impact on prevailing notions of privacy and the otherwise-private individual’s relationship to the public sphere.

C. Reforming the Remedy

The final potential reform would work in tandem with either of the approaches discussed above, and could conceivably address the problem of the “judgment-proof” real perpetrator, a significant policy consideration in tort law generally that has been discussed in connection with online-defamation law in

---

178 Gertz, 418 U.S. at 345 (describing limited-purpose public figures as those who “have thrust themselves to the forefront of particular public controversies in order to influence the resolution of the issues involved”).

179 Id. at 344 (“Public officials and public figures usually enjoy significantly greater access to the channels of effective communication and hence have a more realistic opportunity to counteract false statements than private individuals normally enjoy.”).

180 This combination—no assumption of the risk, but access to media—has not led the Court in the past to conclude that a plaintiff is a public figure. See, e.g., Time, Inc. v. Firestone, 424 U.S. 448, 453–55 (1976) (holding that the plaintiff was not a public figure even though she enjoyed extensive access to media channels). As I argue herein, however, the quirks of the Internet age might lead to a differential balancing of these factors in the online context.

181 See Hutchinson v. Proxmire, 443 U.S. 111, 136 (1979) (clarifying that the media access required for an individual to be considered a public figure is “regular and continuing access to the media”).


183 See, e.g., Stephen G. Gilles, The Judgment-Proof Society, 63 Wash. & Lee L. Rev. 603, 608–09 (2006) (“Millions of low-level torts are committed each year, and those who commit them, regardless of their assets and income, are litigation-proof with regard to these wrongs . . . .”), see also id. at 609 (“The proposition that judgment-proof tortfeasors pose a problem for each of the three leading ‘principled’ accounts of tort law is easily demonstrated.”).
particular. The problem posed by the insolvent defendant might be particularly acute in situations involving online libel because the public at large—including those who may not be identifiable, subject to suit in the United States, or able to compensate the plaintiff for the injuries he has inflicted—enjoys broad access to the Internet medium. This problem undermines both the compensatory and deterrent objectives of modern tort law.

This third reform would effectively tweak the remedy available to plaintiffs in defamation cases, working in combination with either of the first two approaches. The first reform would permit plaintiffs to seek compensation when websites and service providers refuse to investigate or remove allegedly defamatory content and also fail to identify the individual who was originally responsible for posting the material. The second reform would allow plaintiffs to recover against websites and service providers that published defamatory content under the standard common-law framework of distributor and publisher liability, subject, again, to the limitations set forth in New York Times Co. v. Sullivan and its progeny. The twist of the third approach, however, would limit the plaintiff’s recovery in each case to no more than the amount by which the defendant in that case had been unjustly enriched.

Modern web platforms and online publishers frequently track traffic. The lion’s share of these entities derive their principal revenue not from subscriptions, but rather from advertising agreements; the value of these contracts is, in turn, influenced in part by the number of views (or “hits”) a page receives—or, in

---

other words, the number of eyes that the page’s advertisements can reach.\textsuperscript{190} As such, those responsible for managing these companies have a vested financial interest in monitoring traffic on their various pages in order to get a sense of what is and is not effective in attracting a wide readership.\textsuperscript{191} Thus, tracking of traffic and sub-metrics will fall within the scope of many—if not most—business models, and this data can be used to defend against defamation claims.

Provided the defendant tracked traffic and sub-metrics thereof, he would have a reasonable means of calculating precisely how much the defamatory content was worth to him.\textsuperscript{192} Indeed, even if the defendant did not carefully monitor traffic in this manner, publicly available metrics often allow outsiders to approximate the value of a particular page or post.\textsuperscript{193} Under this system, the website or service provider’s incentives to publish the material would exist to a substantially lesser extent, particularly given the fees she could incur through litigation.\textsuperscript{194} Therefore, regardless of the website’s exact tracking technology, a disgorgement remedy could help mitigate the problems posed by the judgment-proof defendant for both the compensatory and deterrence functions of tort law.

There are, of course, possible objections to this approach, as well. The revenue produced by a single visit to the average webpage is tiny,\textsuperscript{195} so unless the defamatory content is published under special circumstances—say, in a post that goes viral, or on a popular website with substantial ad revenues—the typical plaintiff in an online defamation case will be able to win only trivial damages awards. This, in turn, might deter plaintiffs from bringing defamation suits at all. The other side of this coin, however, is that the specter of defamation liability

\begin{footnotes}
\item[190] See Olmstead & Lu, supra note 123; see also PricewaterhouseCoopers LLP \& Interactive Advert. Bureau, supra note 123.
\item[191] See Henry Blodget, Five Years Later, the Huffington Post (and Online Media) Are Coming of Age, BUS. INSIDER (May 18, 2010), http://www.businessinsider.com/huffington-post-comes-of-age-2010-5 (explaining the Huffington Post’s traffic and revenue relative to those of the New York Times, and elaborating on the relationship between the two metrics); Celeste LeCompte, To Fight Ad Blocking, Build Better Ads, NEIMAN REP. (Oct. 26, 2015), http://niemanreports.org/articles/to-fight-ad-blocking-build-better-ads/ (“The growth of ad blocking is a risk for digital media, because it threatens to slash revenues publishers can ill afford to lose.”).
\item[192] See, e.g., Nate Silver, The Economics of Blogging and the Huffington Post, N.Y. TIMES: FIVE THIRTY EIGHT (Feb. 12, 2011, 12:28 PM) (using broad indicators visible to outside evaluators—as opposed to sensitive internal data, which would be far more precise—to estimate the cost, in advertising dollars terms, of the average blog post published on the Huffington Post).
\item[193] See id.; see also, e.g., Mark Hayes, 8 Tools to Research Your Competition, SHOPIFY (June 7, 2012); Your Complete Web Analytics Toolkit, ALEXA, http://www.alexa.com (last visited Nov. 23, 2015).
\item[194] For a discussion of these incentives, see supra notes 120–124 and accompanying text.
\item[195] Kristofer Erickson, Generating Value from the Public Domain, WORLD INTELL. PROP. ORG. MAG., Aug. 2015, at 34, 35 (noting a “commercial estimate that a single visitor to a website is expected to generate USD0.0053 in advertising revenue”).
\end{footnotes}
will likely be less effective at chilling speech online than it is offline, because the expected cost of liability will be comparatively small.\footnote{See supra note 44 and accompanying text.} Thus, the use of this remedy might mitigate one of the dangers that Congress enacted § 230 to avoid in the first place.\footnote{See Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997); see also supra notes 40–44 and accompanying text. An individual may be deterred from speaking if he faces some opposition or threat of injury in response to his speech. Where potential pecuniary damages are minimal, this threat is much less meaningful, and thus less likely to coerce the would-be speaker into remaining silent. Cf. Wendy Seltzer, \textit{Free Speech Unmoored in Copyright’s Safe Harbor: Chilling Effects of the DMCA on the First Amendment}, 24 HARV. J.L.
\& TECH. 171, 184–87 (2010) (discussing the Digital Millennium Copyright Act and the economic incentives that might deter online speech under the statute). This particular remedy admittedly would mean that the legal scheme would retain the odd discrepancy between online and offline defamation liability, albeit perhaps to a lesser degree. See supra Section III.C.2.} In addition, miniscule though the monetary award might be, some recovery is better than no recovery at all, particularly given the fact that this approach also allows plaintiffs the nonpecuniary benefit of vindicating their reputational interests in court.\footnote{See Randall P. Bezanson et al., \textit{Libel Law and the Press: Setting the Record Straight}, 71 IOWA L. REV. 215 (1985) (reporting on the results of a study indicating that most plaintiffs in libel actions bring suit in order to correct misinformation and repair their reputations or to ‘punish the media,’ rather than to secure a money damages award); Robert C. Post, \textit{The Social Foundations of Defamation Law: Reputation and the Constitution}, 74 CALIF. L. REV. 691, 703 (1986) (“From the perspective of an individual who has been dishonored by a libel or slander, the function of defamation law cannot be simply to provide compensation for injuries ‘capable of pecuniary measurement.’ . . . Instead the essential objective of defamation law must be conceived as the restoration of honor.” (footnotes omitted)); see also David S. Ardia, \textit{Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law}, 45 HARV. C.R.-C.L. L. REV. 261, 303–06 (2010); Randall P. Bezanson, \textit{The Libel Suit in Retrospect: What Plaintiffs Want and What Plaintiffs Get}, 74 CALIF. L. REV. 789, 791–92 (1986); James H. Hulme, \textit{Vindicating Reputation: An Alternative to Damages as a Remedy for Defamation}, 30 AM. U. L. REV. 375, 391–413 (1981).} Taken as a whole, while there is room for reasonable minds to disagree about the appropriate line between reputational and speech interests, this third proposed reform would unquestionably improve the current state of affairs if implemented in tandem with one of the first two methods.

\section*{Conclusion}

February 8, 2016 marked the twentieth anniversary of the enactment of the CDA and § 230. During these two decades, the statute has remained static, becoming increasingly out of date against a rapidly evolving technological and cultural backdrop. The Internet has dramatically altered the way that we as a society create, communicate, and consume information, and the current legal framework starkly fails to address the nuances and competing interests at stake in this new era. If modern defamation law is to retain any practical significance in the Internet age, it must be updated to create more constructive economic incentives, yield fairer and more logical results, and better reflect the very real reputa-
tional interests that the current scheme has failed to recognize. The reforms proposed herein would draw upon the realities of the modern technological landscape and the lessons of the last two decades and serve as much-needed first steps toward accomplishing this goal.