UNIVERSITY OF PITTSBURGH LAW REVIEW
Vol. 84 ● Spring 2023

SECTION 230 IN THE POST-COVID ERA: HEALTH MISINFORMATION AND SOCIAL MEDIA

Robert Douglass Kaufman

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

SECTION 230 IN THE POST-COVID ERA: HEALTH MISINFORMATION AND SOCIAL MEDIA

Robert Douglass Kaufman*

INTRODUCTION

Section 230 of the Communications Decency Act of 1996 ("CDA") is one of the most valuable tools for protecting innovation and freedom of expression in cyberspace.[1] It protects online intermediaries, like social media platforms, from being held liable for what other parties post on their forums.[2] As a result, Section 230 has encouraged social media and tech industries to flourish in the United States. Without Section 230, litigation costs from claims that would otherwise be allowed would increase legal fees for internet service providers by up to an estimated 650%.[3]

* J.D., 2023, University of Pittsburgh School of Law; M.M., 2018, Peabody Institute of The Johns Hopkins University; B.M., 2016, Duquesne University. I would like to thank Professor Kevin Abbott for inspiring me to write this Note, and all the members of the University of Pittsburgh School of Law faculty who encouraged me throughout the past three years. I would also like to thank my wife, Hillary, my family, and my friends for their unfailing support. Finally, I would like to thank the inimitable staff of the *University of Pittsburgh Law Review*, without whom I could not have authored this Note.

[1] *Section 230 of the Communications Decency Act*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230 (last visited Oct. 15, 2022); *see also* Ashley Johnson & Daniel Castro, *Overview of Section 230: What It Is, Why It Was Created, and What It Has Achieved*, INFO. TECH. & INNOVATION FOUND. (Feb. 22, 2021), https://itif.org/publications/2021/02/22/overview-section-230-what-it-why-it-was-created-and-what-it-has-achieved.

[2] 47 U.S.C. § 230(c).

[3] Johnson & Castro, *supra* note 1 ("A cost report of litigating claims based on user speech found that the pre-complaint stage can cost a start-up up to $3,000, and the motion-to-dismiss stage can cost $15,000 to $80,000, a significant cost for a small company. But without Section 230 granting start-ups the ability to dismiss cases against them, their legal expenses would pile up even higher, ranging anywhere from $100,000 to $500,000 or more for each case that reaches the discovery stage.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

Section 230 reads:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
> (1) Treatment of publisher or speaker
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
> (2) Civil liability
> No provider or user of an interactive computer service shall be held liable on account of—
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[4]

However, due to a lack of legislation since the early days of the internet and policy-driven judicial adaptations of Section 230's liability exception, service providers have received significantly broader protection than what was originally considered within the scope of the CDA.[5] Because of the safeguards provided by these additional protections, social media platforms have little-to-no external legal impetus to moderate content or limit algorithms that could be damaging to public health and safety.

This problem became ever more apparent during the COVID-19 public health emergency. Algorithms on social media platforms allowed explosive proliferation of health misinformation, limited access to accurate health information, and created a veritable petri dish of health misinformation as the COVID-19 virus spread across the globe.[6] As a result, members of the public refused to heed the advice given by

[4] 47 U.S.C. § 230(c).

[5] Michael D. Smith & Marshall Van Alstyne, *It's Time to Update Section 230*, HARV. BUS. REV. (Aug. 15, 2021), https://hbr.org/2021/08/its-time-to-update-section-230.

[6] Michael A. Gisondi et al., *A Deadly Infodemic: Social Media and the Power of COVID-19 Misinformation*, 24 J. MED. INTERNET RSCH., Feb. 2022 at 1, 2.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

public health officials, and instead listened to the misinformation that had infected their social media feeds.[7]

These problems cannot be answered with more silence. If serious change is not made, social media will continue to be a hotbed of misinformation during the next national emergency. To successfully curb the spread of health misinformation on social media, many different approaches have been considered by social media platforms, Congress, and the courts. This Note will demonstrate that paring back the judicially created protections and returning to a strict textual construction of Section 230 is the best solution for protecting freedom of expression in cyberspace, encouraging more responsible moderation of social media, and preventing the future spread of misinformation during a national crisis.

I. *STRATTON OAKMONT, INC. V. PRODIGY SERVICES, CO.*

Section 230 is a product of the collapse of the fraudulent Stratton Oakmont brokerage house. In *Stratton Oakmont, Inc. v. Prodigy Services, Co.*, Stratton Oakmont sued Prodigy, claiming that Prodigy was liable for content posted by an online bulletin board user.[8] The unidentified user posted libelous statements on Prodigy's popular "Money Talk" bulletin board.[9] Under the standard set forth in *New York Times v. Sullivan*, a plaintiff must show that the defendant exhibited "actual malice" to succeed on a libel claim.[10] However, Prodigy was not the speaker of the libelous statements, but merely the amplifier—i.e., the "distributor." Thus, the case

---

[7] *Id.*

[8] 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1995).

[9] *Id.*

[10] 376 U.S. 254 (1964).

> The constitutional guarantees require, we think, a federal rule that prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with "actual malice"—that is, with knowledge that it was false or with reckless disregard of whether it was false or not.

Id. at 279–80. If the subject of the allegedly libelous statement is not a public figure, the Court held that "the States may define for themselves the appropriate standard of liability for a publisher or broadcaster of defamatory falsehood injurious to a private individual [so long as they do not impose liability without fault]." Gertz v. Robert Welch, Inc., 418 U.S. 323, 347 (1974). However, the Court noted that if a claim is successful under this more lenient standard, punitive damages may not be assessed against the defendant. "In short, the private defamation plaintiff who establishes liability under a less demanding standard than that stated by *New York Times* may recover only such damages as are sufficient to compensate him for actual injury." *Id.* at 350.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

hinged on whether Prodigy was the "publisher" of the libelous statements, and therefore whether Prodigy could be held to the standards set forth by *New York Times*.[11]

The statements at issue in *Stratton Oakmont* included posts claiming that Daniel Porush, Stratton Oakmont's President, "committed criminal and fraudulent acts in connection with the initial public offering of stock of Solomon-Page Ltd."[12] The statements also claimed that the Solomon-Page offering was "a major criminal fraud" and "100% criminal fraud," that Porush was a "soon to be proven criminal," and that Stratton Oakmont was a "cult of brokers who either lie for a living or get fired."[13] The "Money Talk" board on which these statements were posted was the most popular of several online bulletin boards.[14] It had over two million users who would post questions about stocks, investments, and other financial matters.[15] This board—like the other online bulletin boards—was controlled by Prodigy via contracted "Board Leaders" who participated in discussions, promoted board usage, and moderated posts.[16] Prodigy also used a screening software that prescreened all posts containing offensive language.[17]

Stratton Oakmont contended that Prodigy "held itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards, thereby expressly differentiating itself from its competition and likening itself to a newspaper."[18] If—as Stratton Oakmont argued—Prodigy was a "publisher" of defamatory material posted on its online bulletin boards, Prodigy would be subject to liability as if it had originally published that content.[19]

---

[11] *See Stratton Oakmont*, 1995 WL 323710, at *3 (citing Cubby Inc. v. CompuServe Inc., 776 F. Supp. 135, 139 (S.D.N.Y. 1991)).

[12] *Id.* at *1.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.* at *1–3. The Board Leaders were able to send very short explanations to describe their reasoning for removing a post, such as "solicitation, bad advice, insulting, wrong topic, off topic, bad taste, [et cetera]." *Id.*

[17] *Id.* at *2.

[18] *Id.*

[19] *Id.* at *3 (citing Cianci v. New Times Pub. Co., 639 F.2d 54, 61 (2d Cir. 1980); RESTATEMENT (SECOND) OF TORTS § 578 (AM. L. INST. 1977)).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

Alternatively, if the court held that Prodigy did not "publish" the content, but simply acted as a "distributor," it would be considered a passive conduit of that information and would not be liable unless Stratton Oakmont could prove that Prodigy "knew or had reason to know of the defamatory statement at issue."[20]

The *Stratton* court held that Prodigy was not merely a distributor of the libelous information, but that it exercised enough editorial control to be considered a "publisher."[21] As such, liability for the defamatory statements could be imputed to Prodigy. The key distinction that the court pointed to was that Prodigy "held itself out to the public and its members as controlling the content of its computer bulletin boards," and that it "implemented this control through its automatic software screening program, and the Guidelines which Board Leaders are required to enforce."[22] The court also added that even though Prodigy's control is not complete, that fact "does not minimize or eviscerate the simple fact that Prodigy has uniquely arrogated to itself the role of determining what is proper for its members to post and read on its bulletin boards."[23] In promulgating this decision, the court noted that "it appears that this chilling effect [on freedom of communication in cyberspace] is exactly what Prodigy wants, but for the legal liability that attaches to such censorship."[24]

Ironically, the *Stratton Oakmont* decision was responsible for a far more severe chilling effect on online forums than that which the court feared. Because *Stratton Oakmont* held that an "[i]nternet service provider was . . . liable for defamatory statements posted by third parties because it had voluntarily screened and edited some offensive content," service providers who hosted online bulletin boards could now be held liable for attempting to exercise even the slightest control over the content posted on their site.[25] It created a common law catch-22 for internet service providers, penalizing those providers that monitored content published on their

[20] *Id.* at *3 (citing Cubby Inc. v. CompuServe Inc., 776 F. Supp. 135, 139 (S.D.N.Y. 1991)).

[21] *Id.* at *4.

[22] *Id.*

[23] *Id.*

[24] *Id.* at *6.

[25] *See* Shiamili v. Real Est. Grp. of N.Y., Inc., 952 N.E.2d 1011, 1016 (N.Y. 2011) (holding that Section 230 generally immunizes providers from liability for third-party content wherever liability depends on characterizing the provider as a publisher).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

websites, while protecting service providers who turned a blind eye on the content that others uploaded.

II. THE BIRTH OF THE INTERNET AND THE IMPACTS OF SOCIAL MEDIA

For a little perspective, let us take a step backwards. The internet was "born" in 1987, but it was a far cry from the internet we know today.[26] In 1962, the Department of Defense's Advanced Research Projects Agency ("ARPA") began working on a project with the Massachusetts Institute of Technology.[27] This project was a result, in part, of Cold War tensions between the United States and the Union of Soviet Socialist Republics. The project envisioned a decentralized network of computers able to communicate with one another instantly, regardless of distance.[28] Without a central hub responsible for supporting the network, this system would be impervious to any damage that may occur to any single hub, and therefore would be a durable system with significant utility in times of war.[29]

By 1969, ARPA researchers developed "packet switching" technology that allowed computers to receive small amounts of data from other computers, even if there was no direct connection between the computers.[30] This technology allowed ARPA researchers to launch a prototype network called "ARPANET" that connected four computers located at the University of California in Los Angeles, the Augmentation Research Center at Stanford Research Institute, the University of California in Santa Barbara, and the University of Utah School of Computing.[31]

[26] The most recognizable iteration of the early internet was born when the National Science Foundation Network (NSFNet) came online, although more regional "inter-nets" existed before 1987. The Computer Science Network (CSNET) began operations in 1981, and although it was a milestone in the development of the modern internet, it was limited to computer science institutions that could not connect directly to Advanced Research Projects Agency Network (ARPANET). *See NSF and the Birth of the Internet: 1980s*, NAT'L SCI. FOUND., https://www.nsf.gov/news/special_reports/nsf-net/textonly/80s.jsp (last visited Oct. 15, 2022).

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

By the 1970's, ARPANET's capabilities continued to grow, and companies and inventors began to develop smaller but decidedly more powerful computers.[32] These improvements in computing technology began to generate demand for more powerful and publicly accessible computer networks. At that time, networks like ARPANET were only accessible by select universities and institutions that were either able to hook up to ARPANET using tools like Transmission Control Protocol/Internet Protocol ("TCP/IP") or otherwise develop their own networks.[33]

By the 1980's TCP/IP had become the gold standard, making it easier to link discrete networks together, and by 1987, The National Science Foundation Network ("NSFNet") began operating by connecting regional networks to create the first national network of networks, or "inter-net."[34] By 1990, the European Organization for Nuclear Research ("CERN") fellow Tim Berners-Lee developed a new tool to share information using hypertext called the World Wide Web, and on August 6, 1991, the first recognizable webpage was published.[35] Recall that Section 230 of the CDA was enacted in 1996. Seven years later, in August of 2003, Tom Anderson and Chris DeWolfe launched one of the first identifiable modern social media sites, Myspace.[36]

As technology improved, the internet grew into what it is today, and social media took over as an ever-expanding—and increasingly vital—form of communication. This trend continues today. Take, for example, the breadth of Meta's Family of Apps and its recent investment in developing metaverse technology. In Meta's own words:

> The metaverse is a set of digital spaces, including immersive 3D experiences, that are all interconnected so you can easily move between them. It will let you do things you couldn't do in the physical world with people you can't physically be

[32] *NSF and the Birth of the Internet: 1970s*, NAT'L SCI. FOUND., https://www.nsf.gov/news/special_reports/nsf-net/textonly/70s.jsp (last visited Oct. 15, 2022).

[33] *Id.*

[34] *Id.*

[35] *NSF and the Birth of the Internet: 1990s*, NAT'L SCI. FOUND., https://www.nsf.gov/news/special_reports/nsf-net/textonly/90s.jsp (last visited Nov. 8, 2022). The CERN-maintained webpage is available at http://info.cern.ch/hypertext/WWW/TheProject.html. For a thought-provoking exercise, compare the first webpage published in August of 1991 (and still maintained by the European Organization for Nuclear Research) to your Twitter or Facebook feed.

[36] Erik Gregersen, *Myspace*, *in* ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/Myspace (last visited Dec. 27, 2022).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

> with. It will feel like a hybrid of today's online social experiences, sometimes expanded into 3 dimensions or projected into the physical world—and seamlessly stitched together so that you can easily jump from one thing to another.[37]

Although the metaverse seems to have grown from the need for real human interactions where it is otherwise impossible—a need which was dramatically underscored during the COVID-19 global pandemic—plans for metaverse social networking have been in progress for a long time.

Meta's story began in February of 2004 when Mark Zuckerberg launched TheFacebook.com at Harvard University.[38] Facebook grew in popularity during the following years, and by 2008 Facebook had bypassed Myspace to become the most-visited social media website.[39] Facebook developed different forms of social networking, including Messenger, Facebook's interconnected messaging app, and acquired rival social media companies Instagram and WhatsApp.[40] Facebook's Family of Apps diversified into augmented reality and virtual reality with its acquisition of the virtual reality giant, Oculus, in 2014.[41] This growth equipped Facebook—rebranded as Meta on October 28, 2021[42]—for its foray into the world of multiverse social networking.

There are obvious and considerable benefits to social media. Social media allows people to connect with one another in real time, and in a meaningful way, even when they are separated by social, political, geographic, or medical barriers. And there is no doubt the metaverse will continue to revolutionize the ways in which we are able to learn to work, play, and communicate with one another. But for all the advantages social media has to offer, it can also present significant dangers. As we have seen in recent years, algorithmic interference on social media creates a

---

[37] *How Will Metaverse Change Your World?*, META, https://www.facebook.com/business/news/let-me-explain-episode-metaverse (last visited Oct. 15, 2022).

[38] Mark Hall, *Facebook*, *in* ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/Facebook (last visited Oct. 15, 2022).

[39] *Id.*

[40] *Id.*

[41] *See* Riyado Sofian, *Meta: It's Only a Meta of Time*, SEEKING ALPHA (Oct. 2, 2022, 4:39 AM), https://seekingalpha.com/article/4544227-meta-its-only-a-meta-of-time.

[42] *Introducing Meta: A Social Technology Company*, META (Oct. 28, 2021), https://about.fb.com/news/2021/10/facebook-company-is-now-meta.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

revolving amalgam of information and misinformation which is at least partially responsible for creating an increasingly polarized and politicized cyberspace.[43]

Broadly speaking, social media algorithms are essential tools for ensuring that users are shown material that is interesting to them, connecting users with others that they may know, and generating relevant geo-targeted advertisements for each user.[44] Each platform's unique algorithms use millions of data points, including the user's search history, the user's interactions with posts, the amount of screen time a post or ad receives, and even data from off-app activity.[45] As a result of the algorithms' interactions with a user's activity, a type of individualized feedback loop occurs to create a virtual world for the user to enjoy each time they log in.[46] It creates a unique, personally tailored user experience for each and every user.[47] A user's feed will begin showing them things that they like, which typically elicits a user reaction that in turn affects the algorithm.[48] This feedback loop continues in perpetuity so that the user's experience on the site remains current with that user's interests.[49]

For better or worse, social media sites thrive off their addictive quality, and this addiction is naturally driven by the efficacy of each site's closely guarded algorithms.[50] And because social media sites generally make their money from ad revenue, the longer a site can keep a user engaged, the more money the site makes,

---

[43] Paul Barrett et al., *How Tech Platforms Fuel U.S. Political Polarization and What Government Can Do About It*, BROOKINGS (Sept. 27, 2021), https://www.brookings.edu/blog/techtank/2021/09/27/how-tech-platforms-fuel-u-s-political-polarization-and-what-government-can-do-about-it/.

[44] *See generally* Ro'ee Levy, *Social Media, News Consumption, and Polarization: Evidence from a Field Experiment*, 111 AM. ECON. REV. 831, 870 (2021).

[45] *Id.*; *see also* Will Oremus et al., *Facebook Under Fire: How Facebook Shapes Your Feed*, WASH. POST (Oct. 26, 2021, 7:00 AM), https://www.washingtonpost.com/technology/interactive/2021/how-facebook-algorithm-works/.

[46] Oremus et al., *supra* note 45.

[47] *Id.*

[48] *Id.*

[49] Although many people consume news on social media in a way that reinforces their viewpoints, thus perpetuating the feedback loop, it appears that the algorithms can be relatively easily manipulated by the user. However, this only occurs if the user repeatedly interacts with "counter-attitudinal" content. Levy, *supra* note 44, at 834.

[50] Tammy Qiu, *A Psychiatrist's Perspective on Social Media Algorithms and Mental Health*, HAI STAN. UNIV. (Sept. 14, 2021), https://hai.stanford.edu/news/psychiatrists-perspective-social-media-algorithms-and-mental-health.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

thereby incentivizing hyper-addictive, algorithm-generated feedback loops.[51] A balanced, neutral algorithm will show the user a variety of content from differing viewpoints. However, when a non-neutral algorithm is repeatedly fed similar inputs, the algorithm will tailor the user's experience to an extreme, creating a user experience that continually polarizes the content that the user views until the algorithm shuts out other viewpoints completely.[52]

Hypothetically, let's say that your partner loves dachshunds. While you are browsing Instagram's "Reels," you come across a video of a dachshund, "like" the video, and send that video to your partner. Later that day, as you are once again scrolling through Instagram, you like a couple more dog videos and photos that tumble across your screen. The next day, your Reels—originally dominated by music, sports, and food—now have the occasional dog video. The day after that, one of these dog videos stars another dachshund, and again you send it to your partner and like that video. By the next week, you realize that your Reels are more than half dogs, a quarter of which are dachshunds. Continue this cycle for a few more weeks, and your feed will become a veritable dachshund dashboard.[53]

In some cases, the effect of the algorithm's feedback loop is limited to providing the user with an endless supply of adorable dog videos, but in other cases it can produce real-life consequences—both good and bad. Take, for example, the 2014 "Ice Bucket Challenge" that resulted in 2.4 million user-created videos and over $220 million dollars raised for ALS research during the months of July and August.[54] On the flip side, we can see the impact of algorithms on misinformation in the January 6 Capitol Riot that was spurred, in part, by misinformation spread by President Donald Trump and circulated among highly polarized social media groups on Facebook, Twitter, Parler, and 4chan.[55]

---

[51] Kalev Leetaru, *What Does It Mean for Social Media Platforms to "Sell" Our Data?*, FORBES (Dec. 15, 2018, 3:56 PM), https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=64e3b61f2d6c.

[52] Barrett et al., *supra* note 43.

[53] For better or worse, this hypothetical is less than hypothetical to the author of this Note.

[54] *Pete Frates, Man Who Championed ALS Ice Bucket Challenge, Dies*, AL JAZEERA (Dec. 9, 2019), https://www.aljazeera.com/news/2019/12/9/pete-frates-man-who-championed-als-ice-bucket-challenge-dies.

[55] *See* Nicholas Wu, *Jan. 6 Investigators Demand Records from Social Media Companies*, POLITICO (Aug. 27, 2021, 1:51 PM), https://www.politico.com/news/2021/08/27/jan-6-investigation-social-media-records-506936.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

During the height of the COVID-19 pandemic, algorithms prioritized certain types of health information—and misinformation—to the exclusion of others, again all on a highly user-dependent basis.[56] Some algorithms were geared to show users more interesting and sensational posts at the expense of posts that were medically accurate.[57] And when non-neutral feedback loops mixed with health misinformation and hoax posts, misinformation about the virus and efficacy of vaccines exploded across social media platforms. Interestingly, almost all of this misinformation originated from only twelve individuals.[58] Posts directly created by these individuals and shared by others made up over 65% of extant health misinformation on social media, and the other 35% of health misinformation overwhelmingly mimicked or rephrased that which had been shared previously by those twelve users.[59] Because the algorithms prioritized this misinformation to the exclusion of accurate health information, many people began to believe that these hoax posts were true, greatly impacting vaccination rates in the United States.[60]

But these dangers extend beyond medical misinformation, most recently to interference with fair democratic elections.[61] Nearly half of Americans consume some level of news from social media sites,[62] no doubt because of the significant advantages of speed and interactivity that social media news feeds have over traditional news media. Some of these hoax posts can be avoided by a discerning reader, but the fact that an algorithm controls what information a user can or cannot see, thereby limiting what information that user is able to easily consume, is

[56] U.S. SURGEON GEN., CONFRONTING HEALTH MISINFORMATION: U.S. SURGEON GENERAL'S ADVISORY ON BUILDING A HEALTHY INFORMATION ENVIRONMENT (2021).

[57] *Id.*

[58] Shannon Bond, *Just 12 People Are Behind Most Vaccine Hoaxes on Social Media, Research Shows*, NPR (May 14, 2021, 11:48 AM), https://www.npr.org/2021/05/13/996570855/disinformation-dozen-test-facebooks-twitters-ability-to-curb-vaccine-hoaxes.

[59] *Id.*

[60] *See generally* Renee Garett & Sean D. Young, *Online Misinformation and Vaccine Hesitancy*, 11 TRANSNAT'L BEHAV. MED. 2194, 2199 (2021).

[61] *See generally* Mekela Panditharatne et al., *Information Gaps and Misinformation in the 2022 Elections*, BRENNAN CTR. FOR JUST. (Aug. 2, 2022), https://www.brennancenter.org/our-work/research-reports/information-gaps-and-misinformation-2022-elections.

[62] Amy Mitchell & Jacob Liedke, *About Four-In-Ten Americans Say Social Media Is an Important Way of Following COVID-19 News*, PEW RSCH. CTR. (Aug. 24, 2021), https://www.pewresearch.org/fact-tank/2021/08/24/about-four-in-ten-americans-say-social-media-is-an-important-way-of-following-covid-19-vaccine-news/.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

exceedingly dangerous to the general public.[63] Because of these algorithms, misinformation is not screened out or, in some cases, even diluted by reputable information.[64] Instead, social media algorithms can create a concentrated stream of sensational information, convincing some users that misinformation is true, and thereby impacting overall public health and safety.

Algorithms can quickly amplify already sensational misinformation. However, because Section 230's broad shield currently protects social media sites from nearly any liability, and because the courts and Congress have failed to update Section 230 as technology improved, social media companies have little incentive to address these problems. In fact, because of the nature of ad revenue and because social media platforms cannot be held liable for failing to remove or limit misinformation, these sites can only stand to benefit from the proliferation of sensational posts.

III. THE COMMUNICATIONS DECENCY ACT AND SECTION 230'S BROAD INTERPRETATIONS

In 1996, one year after *Stratton Oakmont*, Congress decided to address the *Stratton* court's misstep and take action to encourage service providers to censor and control their own sites.[65] To do so, Congress needed to eliminate the liability *Stratton*

[63] *See* Amy Mitchell et al., *Americans Who Mainly Get Their News on Social Media Are Less Engaged, Less Knowledgeable*, PEW RSCH. CTR. (July 30, 2020) (finding that U.S. adults who get their news on social media are "less likely than other news consumers to closely follow major news stories, such as the coronavirus outbreak and the 2020 presidential election. And, perhaps tied to that, this group also tends to be less knowledgeable about these topics").

[64] Levy, *supra* note 44, at 834 ("On the one hand, Facebook's algorithm seems to filter counter-attitudinal news, probably since it attempts to personalize news based on the user's behavior and perceived interests. While it is not possible to estimate the effect of specific posts filtered by the algorithm, I show that exposure to counter-attitudinal news decreases affective polarization. This suggests that social media algorithms may be increasing polarization.").

[65] Recall that the Communications Decency Act—and, most importantly, Section 230—was enacted only five years after the first website was published, and seven years before the world saw the first modern social media platform come into existence. *See* Section II, *supra*.

For insight into the recognized uses and capabilities of the internet as of 1997, see the introductory discussion of how the internet functions in *Reno v. Am. Civ. Liberties Union*:

> Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail (e-mail), automatic mailing list services . . . , "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

> tools constitute a unique medium—known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.
>
> E-mail enables an individual to send an electronic message—generally akin to a note or letter—to another individual or to a group of addressees. The message is generally stored electronically, sometimes waiting for the recipient to check her "mailbox" and sometimes making its receipt known through some type of prompt. A mail exploder is a sort of e-mail group. Subscribers can send messages to a common e-mail address, which then forwards the message to the group's other subscribers. Newsgroups also serve groups of regular participants, but these postings may be read by others as well. There are thousands of such groups, each serving to foster an exchange of information or opinion on a particular topic running the gamut from, say, the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls. About 100,000 new messages are posted every day. In most newsgroups, postings are automatically purged at regular intervals. In addition to posting a message that can be read later, two or more individuals wishing to communicate more immediately can enter a chat room to engage in real-time dialogue—in other words, by typing messages to one another that appear almost immediately on the others' computer screens. The District Court found that at any given time "tens of thousands of users are engaging in conversations on a huge range of subjects." It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought."
>
> The best-known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. Some of these documents are simply files containing information. However, more elaborate documents, commonly known as Web "pages," are also prevalent. Each has its own address—"rather like a telephone number." Web pages frequently contain information and sometimes allow the viewer to communicate with the page's (or "site's") author. They generally also contain "links" to other documents created by that site's author or to other (generally) related sites. Typically, the links are either blue or underlined text—sometimes images.
>
> Navigating the Web is relatively straightforward. A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links. Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.

Reno v. Am. Civ. Liberties Union, 521 U.S. 844, 851–53 (1997).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

Oakmont placed on service providers for good faith editing and removal of user posts. The resulting Section 230 has two parallel goals: "[T]o promote the free exchange of information and ideas over the Internet and to encourage voluntary monitoring for offensive or obscene material."[66]

Section 230 has outshone the rest of the CDA in the years since it was enacted. In its original form, the CDA was designed to place liability on online speech.[67] Section 230, on the other hand, is simply an exception that protects any "provider or user of an interactive computer service" from liability resulting from "any action taken in good faith to restrict access to or availability of material . . . consider[ed] to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."[68]

It is important to note that although Section 230 itself has not been interpreted by the Supreme Court, portions of the CDA were challenged and overturned in *Reno v. American Civil Liberties Union*.[69] In *Reno*, the ACLU and several other activist groups including Human Rights Watch, Planned Parenthood, Electronic Frontier Foundation, and Electronic Privacy Information Center challenged the constitutionality of provisions of the CDA that were intended to protect minors from accessing harmful material on the internet.[70]

Specifically, *Reno* held that (1) provisions of the CDA prohibiting transmission of obscene, indecent or patently offensive communications to persons under eighteen were content-based blanket restrictions on speech and could not be analyzed as a form of time, place, and manner regulation; (2) the challenged provisions were facially overbroad in violation of the First Amendment; and (3) the constitutionality of the provisions would be saved by severing "or indecent" from the statute.[71] In concluding that the language of Section 223(a) and (d) was overly broad and violative of the First Amendment, the Court construed the word "indecent"[72] and the

[66] Shiamili v. Real Est. Grp. N.Y., 952 N.E.2d 1011, 1016 (N.Y. 2011) (quoting Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1099-1100 (9th Cir. 2009)).

[67] Communications Decency Act of 1996, PUB. L. NO. 104-104, 110 Stat. 56 (codified at 47 U.S.C. § 230).

[68] 47 U.S.C. § 230(c).

[69] *Reno*, 521 U.S. at 849.

[70] *Id.* at 844.

[71] *See id.* at 864–85.

[72] *Id.*; *see also* 47 U.S.C. § 223(a).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

phrase "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs."[73] The Court found that "the CDA . . . presents a greater threat of censoring speech that, in fact, falls outside the statute's scope. Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection."[74]

Since that time, Section 230 has been interpreted by lower courts as extending to social media providers something close to a general immunity from liability for any content posted to a social media site by third parties.[75] Although courts differ in their interpretations of Section 230, it is generally interpreted as creating a three-prong test to determine whether dismissal of a claim is mandated.[76] These prongs require a court to determine whether: (1) the defendant is a "provider or user of an interactive computer service," (2) the information in question is "information

[73] *Reno*, 521 U.S. at 845.

[74] *Id.* at 874.

> Under the CDA, a parent allowing her 17-year-old to use the family computer to obtain information on the Internet that she, in her parental judgment, deems appropriate could face a lengthy prison term. Similarly, a parent who sent his 17-year-old college freshman information on birth control via e-mail could be incarcerated even though neither he, his child, nor anyone in their home community found the material "indecent" or "patently offensive," if the college town's community thought otherwise.

Id. at 878.

[75] *See, e.g.*, Shiamili v. Real Est. Grp. N.Y., 952 N.E.2d 1011, 1016–18 (N.Y. 2011) ("[Courts] have generally interpreted Section 230 immunity broadly, so as to effectuate Congress's policy choice . . . . Consistent with this view, we read section 230 to bar lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content."); Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997) ("Congress made a policy choice . . . not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages."); *see also* Enigma Software Grp. v. Malwarebytes, Inc., 946 F.3d 1040 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 13 (2020); Biden v. Knight First Amend. Inst. Colum. Univ., 926 F.3d 226 (2d Cir. 2019), *cert. denied*, 141 S. Ct. 1220 (2021).

[76] *See* Klayman v. Zuckerberg, 753 F.3d 1354, 1357–60 (D.C. Cir. 2014) ("The Communications Decency Act mandates dismissal if (i) Facebook is a 'provider or user of an interactive computer service,' (ii) the information for which Klayman seeks to hold Facebook liable was 'information provided by another information content provider,' and (iii) the complaint seeks to hold Facebook liable as the 'publisher or speaker' of that information. We hold that, on the face of this complaint, all three prongs of that test are satisfied." (citations omitted)).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

provided by another information content provider," and (3) the complaint seeks to hold the defendant liable as the "publisher or speaker" of that information.[77]

The Fourth Circuit was one of the first federal appellate courts to address the liability issues of the revised Section 230.[78] In *Zeran v. America Online, Inc.*, plaintiff Kenneth Zeran sued AOL for unreasonable delay in removing defamatory messages posted by a third party.[79] On April 25, 1995, an unidentified third party posted a message that advertised T-shirts emblazoned with tasteless messages about the 1995 Oklahoma City bombing and instructed interested buyers to call "Ken" at Zeran's home phone number.[80] After receiving a large volume of harassing and threatening phone calls, Zeran contacted AOL and requested that AOL take remedial action to stop the harassment.[81] AOL assured Zeran that the posts would be removed but refused to post a retraction.[82]

Over the next five days, an unknown third party posted similar messages advertising other tasteless T-shirts, bumper stickers, and key chains, again directing buyers to call "Ken" at Zeran's home phone number, and requesting that callers should "please call back if busy."[83] Zeran repeatedly contacted AOL requesting that action be taken and reported the incident to the FBI.[84] By April 30, Zeran was receiving abusive and threatening calls at his home phone number—which he also used for business purposes—at a frequency of approximately one call every two minutes; the number of calls subsided to fifteen per day by May 14.[85]

Before the Fourth Circuit, Zeran asserted that AOL should be held liable for "defamatory speech initiated by a third party," arguing that, after being notified of the defamatory posts, "AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future

[77] 47 U.S.C. § 230(c).

[78] *Zeran*, 129 F.3d at 328.

[79] *Id.*

[80] *Id.* at 329.

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

defamatory material."[86] In response, AOL argued that Congress immunized service providers from this type of tort liability under Section 230.[87]

The Fourth Circuit analyzed the text of Section 230 and concluded that its "plain language . . . creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, [Section] 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role."[88] The court continued, "Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet," and "[t]he imposition of tort liability on service providers for the communications of others represented . . . simply another form of intrusive government regulation of speech."[89]

In taking this approach, the court blended the subtle distinctions between publisher, speaker, and distributor liability. The *Zeran* court held not only that a service provider was protected from being treated as a "publisher or speaker of any information provided by another information content provider,"[90] but that Section 230 should be reasonably expanded to cover distributor liability because it would not be feasible for internet service providers to conduct due diligence on the services that they provide.[91] Thus, as a matter of law, a service provider is considered a neutral distributor of information unless the plaintiff can show that the provider acted in bad faith. And even then, in the case of a defamation claim, the plaintiff still must pass the onerous standard set by *New York Times v. Sullivan*.[92]

---

[86] *Id.* at 330.

[87] *Id.*

[88] *Id.* Specifically, the text at issue in this case comes from 47 U.S.C. § 230(c)(1), which states, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

[89] *Zeran*, 129 F.3d at 330.

[90] 47 U.S.C. § 230(c)(1).

[91] *Zeran*, 129 F.3d at 333 ("If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context.").

[92] 376 U.S. 254, 279–80 (1964).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

Numerous other courts have adopted this expansive view and have left us with a version of Section 230 that falls short of imposing almost any liability, even where service providers are on notice that harmful information has been posted on their sites.[93] But Section 230 has expanded beyond this: courts have extended the protections to apply to product-defect claims,[94] claims against CEOs of tech companies,[95] and nearly any actions taken to remove or edit content.[96]

Because of these extremely generous readings of Section 230, the statute could be reasonably interpreted to impose "no limits on an Internet company's discretion to take down material," as pointed out by Justice Thomas in his concurrence in *Malwarebytes v. Enigma Software Group*.[97] Justice Thomas goes on to acknowledge the jarring impact of the majority's decision to deny certiorari in the *Malwarebytes* case stating, "[Section] 230 now apparently protects companies who racially discriminate in removing content."[98] In its current form, Section 230 protects a service provider from liability for nearly any content posted on its site, even if the provider has knowledge of the illegality or harmfulness of such content, and even if its algorithms interfere with who can or cannot see that content.[99]

One of the only types of content moderation that would be denied Section 230's immunity is moderation that might have an anticompetitive purpose. In *Malwarebytes v. Enigma Software Group*, the Ninth Circuit analyzed the language

---

[93] *See* Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 420 (1st Cir. 2007) ("It is, by now, well established that notice of the unlawful nature of the information provided is not enough to make it the service provider's own speech. We confirm that view and join the other courts that have held that Section 230 immunity applies even after notice of the potentially unlawful nature of the third-party content.") (citations omitted); *see also* Johnson v. Arden, 614 F.3d 785, 791 (8th Cir. 2010); Doe v. MySpace, Inc., 528 F.3d 413, 418 (5th Cir. 2008); Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1321 (11th Cir. 2006) ("The majority of federal circuits have interpreted the CDA to establish broad federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.") (citations and quotations omitted).

[94] Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12 (1st Cir. 2016).

[95] Klayman v. Zuckerberg, 753 F.3d 1354 (D.C. Cir. 2014).

[96] Malwarebytes, Inc. v. Enigma Software Grp., 141 S. Ct. 13, 16–17 (2020).

[97] *Id.* at 17.

[98] *Id.*

[99] Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Sec. 230 Immunity*, 86 FORDHAM L. REV. 401, 406–07 (2017) ("Courts have built a mighty fortress protecting platforms from accountability for unlawful activity on their systems—even when they actively encourage such activity or intentionally refuse to address it.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

of Section 230(c)(2).[100] Section 230(c)(2) states, "No provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or *otherwise objectionable*, whether or not such material is constitutionally protected."[101] Although the language of Section 230 has regularly been read to protect free speech on the internet at all costs, the Ninth Circuit held that a service provider's immunity was not limitless, but that "the phrase 'otherwise objectionable' does not include software that the provider finds objectionable for anticompetitive purposes."[102]

As Justice Thomas wisely notes in his concurrence, "The decision is one of the few where courts have relied on purpose and policy to *deny* immunity under [Section] 230. But the court's decision to stress purpose and policy is familiar. Courts have long emphasized nontextual arguments when interpreting [Section] 230, leaving questionable precedent in their wake."[103] Ultimately, the question remains: what can be done to clarify the law and remedy the questionable precedent left by the lack of guidance by the Supreme Court?

IV. WHAT MUST BE DONE

With the expansive and questionable precedent left by the circuits and the very real possibility of another national crisis that could be influenced by misinformation on social media, change is desperately needed. There are three ways possible ways that reform could occur: through self-regulation by social media platforms; through legislative amendment of Section 230; and by judicial intervention.

A. Self-Regulation

Tech advocates and social media companies regularly take the position set forth by the Fourth Circuit in *Zeran* and its progeny, claiming that the only reasonable way

[100] *Malwarebytes, Inc.*, 141 S. Ct. at 17.

[101] 47 U.S.C. § 230(c)(2) (emphasis added).

[102] Enigma Software Grp. v. Malwarebytes, Inc., 946 F.3d 1040, 1045 (9th Cir. 2020) (citing 47 U.S.C. § 230(c)(2)).

[103] *Malwarebytes, Inc.*, 141 S. Ct. at 14.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

to deal with the deficiencies of Section 230 is through self-regulation.[104] According to many service providers, Section 230's shield is necessary because it would be unfeasible for the providers to filter, evaluate, and react to every post made by billions of users if they were mandated to do so.[105] Advocating for this broad shield usually requires adopting the position that the internet's mere existence relies upon Section 230's broad protections: assuming social media sites would be unable to host any user-generated content for fear of liability if Section 230 did not exist in its current form, and any paring back of Section 230's broad protections would result in highly restricted speech online.[106]

While it is true that Section 230 is, in part, responsible for the explosive growth of technology and social media in the United States, this argument is problematic. The claim that it would be unreasonable for a social media company to filter posts on its platform was first voiced in *Zeran*.[107] However, recently celebrating its twenty-fifth anniversary, *Zeran* is not a new or even recent case. Although the number of users who are active on social media has increased over time, technology has also developed dramatically, requiring much less manpower to screen potentially detrimental posts.[108] Moreover, this stance contradicts the claims of the same advocates who argue that social media sites are fully capable of handling misinformation without any need for external regulation; a social media platform cannot be simultaneously overwhelmed by the amount of users on its site and fully capable of responsibly moderating posts for harmful content.

One advocate for self-regulation is Meta CEO Mark Zuckerberg, who believes platforms like Facebook and Instagram are fully capable of filtering out health misinformation by: "putting [authoritative COVID-19 information] at the top of Facebook and Instagram;" having a page that links to Facebook's vaccine access tool; removing content "that could lead to imminent harm" and flagging "content

[104] *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) ("Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context.").

[105] Johnson & Castro, *supra* note 1.

[106] *Id.*

[107] *Zeran*, 129 F.3d at 331.

[108] Rem Darbinyan, *The Growing Role of AI in Content Moderation*, FORBES (June 14, 2022, 6:45 AM), https://www.forbes.com/sites/forbestechcouncil/2022/06/14/the-growing-role-of-ai-in-content-moderation/?sh=17994cb74a17.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

that our fact checkers flag as misinformation."[109] Beyond this, Meta has taken self-regulation one step further by creating an Oversight Board "to help Facebook [and Instagram] answer some of the most difficult questions around freedom of expression online: what to take down, what to leave up, and why."[110]

The Oversight Board offers an interesting example of where the future of social media regulation could be headed. The purpose of the Oversight Board is:

> To protect free expression by making principled, independent decisions about important pieces of content and by issuing policy advisory opinions on Meta's content policies. The board will operate transparently and its reasoning will be explained clearly to the public, while respecting the privacy and confidentiality of the people who use Meta Platforms, Inc.'s services, including Facebook and Instagram . . . . It will provide an accessible opportunity for people to request its review and be heard.[111]

The Oversight Board functions like a quasi-agency; it currently includes twenty-three members from various professions, backgrounds, and nationalities,[112] selects the cases to be reviewed, issues binding decisions on user appeals, and makes policy recommendations to Facebook and Instagram.[113]

And, in an effort to maintain its impartiality, Meta created an independent irrevocable trust to govern the Oversight Board.[114] Meta funds the trust and appoints trustees while the trust, in turn, maintains and approves the board's operating budget, and appoints and removes Oversight Board members.[115] The Oversight Board is not

[109] Casey Newton, *Mark in the Metaverse*, THE VERGE (July 22, 2021), https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview?scrolla=5eb6d68b7fedc32c19ef33b4.

[110] OVERSIGHT BOARD, https://oversightboard.com/ (last visited Oct. 15, 2022).

[111] OVERSIGHT BOARD, *Introduction*, *in* OVERSIGHT BOARD CHARTER, Introduction (2023) [hereinafter CHARTER].

[112] *Meet the Board*, OVERSIGHT BOARD, https://www.oversightboard.com/meet-the-board/ (last visited Mar. 8, 2023).

[113] *Appeal to shape the future of Facebook and Instagram*, OVERSIGHT BOARD, https://oversightboard.com/appeals-process/ (last visited Mar. 8, 2023).

[114] CHARTER, *supra* note 111.

[115] *Id.*, art. 5, § 2.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

directly controlled by Meta, but instead contracts with it for its services.[116] Meta maintains that it is committed "to the board's independent oversight on content decisions and the implementation of those decisions."[117]

These efforts are a step in the right direction, but they are not enough. Facebook's efforts to promote "authoritative information" alone cannot outweigh the influence that its algorithm has on users when that algorithm simultaneously screens out reputable health information, and there has been no apparent effort to change this paradox. Additionally, the Oversight Board only moderates content on Facebook and Instagram and, even then, it does so in a highly methodical fashion—and perhaps more importantly, it is only able to do so retroactively.[118] Assuming that the Oversight Board is as effective as Meta claims, it still has no impact on any other platforms, and it has absolutely no impact on Facebook's or Instagram's algorithms beyond its ability to make "policy recommendations."[119] Regardless, the Oversight Board would not be liable under Section 230 if it chose not to remove a harmful post, even if it had been given notice of that post's harmful content.[120]

One possible solution for self-moderation could be establishing a universal oversight board with input from all major social media platforms.[121] Meta has already recognized this possibility. When Meta created the Oversight Board's trust, it empowered the trust to receive funding from outside sources, creating the potential for a universal oversight board and platform-specific boards that oversee content

[116] *Id.*, art. 5, § 1.

[117] *Id.*, art. 5, § 3.

[118] The appeals process takes "a few weeks" for the Oversight Board to select "just a handful [of appeals] per month" to review, of the "thousands of appeals per week" that they receive. After an appeal is selected for review, the review of Facebook or Instagram's decision "[m]ight take up to 3 months." In reality any given post has a slim chance of getting picked for actual review. If it is one of the lucky ones, the process may still take a total of nearly four months. *Appeal to Shape the Future of Facebook and Instagram*, OVERSIGHT BOARD, https://oversightboard.com/appeals-process/ (last visited on Oct. 15, 2022).

[119] *See id.*; CHARTER, *supra* note 111, art. 5 § 1.

[120] *See supra* Section III.

[121] Such an organization could be multi-tiered, like the United States Judicial system, with one universal oversight board at the top, dictating policy and deciding only the most important appeals; a series of appellate boards, each governing a specific social media platform or type of platform; and the lowest level boards deciding appeals in the first instance.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

moderation among and across major social media platforms.[122] If all major social media companies could agree on the level of control that a universal oversight board might have over each platform—including, importantly, actual control over algorithms and ethical content moderation—such a universal oversight board (or system of oversight boards) might have a very real impact on misinformation.

But realistically, a universal oversight board would be ineffective at achieving these goals. Although expansion of the Oversight Board would offer consistent, neutral content moderation among and across major social media platforms, the Oversight Board still would have no say on the programming of algorithms, and it is unlikely that any social media company would permit an organization like the Oversight Board to effect those changes. At best, a universal oversight board could make policy recommendations and respond to user appeals, just like the Oversight Board currently does for Facebook and Instagram.[123]

Even if major social media companies agreed to establish a universal oversight board that impartially moderated content—and algorithms—there would be no external impetus for change, and there would be nothing holding the universal oversight board itself accountable. Social media companies would have no real incentive to join the universal oversight board or agree to be bound by its decisions, and start-ups with minimal resources would have even less motivation to join it. Beyond this, even if all social media platforms would be willing to be bound by a universal oversight board, both the general operating expenses and the amount of data that would need to be processed would be astronomical. If a single social media company cannot filter every post on its platform, it would be virtually impossible for a third party to filter the posts from all of the world's social media platforms without shouldering a truly colossal expense.

Although Meta's Oversight Board offers an exemplary illustration of transparency, self-regulation, and content moderation, there has yet to be an effective solution offered by any social media platform that could directly challenge the proliferation of misinformation at its core, and it seems unlikely that such a solution could ever be effective as to all major social media platforms.

---

[122] Issie Lapowsky, *Facebook Tells Us how Its New Board Will Oversee Mark Zuckerberg*, PROTOCOL (May 6, 2020), https://www.protocol.com/facebook-oversight-board-interview (Meta officer stating that "the trust allows for more than just Facebook to contribute funding").

[123] *See* CHARTER, *supra* note 111, art. 5, § 1.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

B. Legislative Amendment

In lieu of an effective response from social media companies, Congress could update the CDA to respond to the significant changes in technology over the past twenty-five years. If the goal of the CDA is "to promote the free exchange of information and ideas over the Internet and to encourage voluntary monitoring for offensive or obscene material,"[124] it would be reasonable for Congress to reexamine the CDA, given the exponential growth of the internet, to further those goals.

Proposals from both sides of the aisle have aimed to amend the CDA. For example, Democrat Amy Klobuchar's Health Misinformation Act of 2021 ("HMA"), S. 2448, would limit the protections of Section 230 and would provide that, under some circumstances, a social media site that allows for proliferation of health misinformation without proper limitation would lose its Section 230(c) protection.[125] Specifically, the HMA amends the CDA to provide that, under specific circumstances, a service provider that allows "for the proliferation of health misinformation through that service" to be treated as the publisher or speaker of that misinformation.[126] The HMA's amended Section 230 would read as follows:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
> (1) Treatment of publisher or speaker
> ***(A) IN GENERAL.—Except as provided in subparagraph (B), no provider*** or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
> ***(B) Exception.—A provider of an interactive computer service shall be treated as the publisher or speaker of health misinformation that is created or developed through the interactive computer service during a covered period if the provider promotes that health misinformation through an algorithm used by the provider (or similar software functionality), except that this subparagraph shall not apply if that promotion occurs through a neutral mechanism, such as through the use of chronological functionality . . .***[127]
> (2) Civil liability

[124] Shiamili v. Real Est. Grp. N.Y., 952 N.E.2d 1011, 1016 (N.Y. 2011).

[125] 47 U.S.C. § 230(c); Health Misinformation Act of 2021, S. 2448, 117th Cong. (2021).

[126] Health Misinformation Act of 2021, S. 2448, 117th Cong. (2021).

[127] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[128]

The HMA defines "covered period" in subsection (f): "The term 'covered period' means a period during which a public health emergency declared by the Secretary of Health and Human Services under Section 319 of the Public Health Service Act (42 U.S.C. [§ 247(d)]), including a renewal of any such declaration, is in effect."[129]

This amendment would keep Section 230 functioning just as it does today, with the obvious caveat that if a service provider promotes health misinformation through a non-neutral algorithm during a public health emergency, that service provider will be treated as the speaker or publisher of that misinformation instead of a neutral distributor. In sum, the HMA would increase the threat of civil liability and encourage social media sites to take appropriate action to prevent the spread of harmful health misinformation when it matters most.

Although this would be an effective response to the immediate problem of health misinformation during a pandemic, it would have no effect if there is no "public health emergency declared by the Secretary of Health and Human Services under Section 319 of the Public Health Service Act."[130] At best, this amendment is a bandage that will inevitably fall off—it has no teeth unless a public health emergency is declared, and even then it would have no impact on misinformation disseminated during other national emergencies. Ultimately, although the HMA might have succeeded at addressing the immediate problem of health misinformation during the COVID-19 health emergency, it would do nothing to address the overarching issues with Section 230 liability in any other context.

---

[128] 47 U.S.C. § 230(c)(2).

[129] Health Misinformation Act of 2021, S. 2448, 117th Cong. (2021).

[130] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

Another amendment, proposed by Republican Josh Hawley, is the Ending Support for Internet Censorship Act (ESICA), S. 1914, which would force any interactive social media site that has either significant usership or generates over $500 million in global annual revenue to be audited for partisan bias to keep their legal immunity under Section 230.[131] ESICA would put the burden of proof on qualifying social media companies to show "by clear and convincing evidence that the provider does not . . . moderate information provided by other information content providers in a politically biased manner."[132] ESICA further defines the moderation practices of a service provider as "politically biased moderation" if the provider moderates content in a manner that "is designed to negatively affect a political party, political candidate, or political viewpoint," or that "disproportionately restricts or promotes access to, or the availability of, information from a political party, political candidate, or political viewpoint."[133] Additionally, politically biased moderation could include decisions made by an officer or employee "about moderating information provided by other information content providers that is motivated by an intent to negatively affect a political party, political candidate, or political viewpoint."[134]

Accordingly, ESICA would (1) remove the protections of Section 230 from large platforms until the platforms could prove that they are moderating content in an unbiased way; (2) impose greater liability if any employee moderates in a way that could be interpreted as politically motivated; and (3) create a significant challenge for algorithmic moderation to prevent inadvertent politically biased moderation.

But not only would ESICA fail to solve the most pressing problems presented by Section 230, it would prevent platforms from censoring or removing political candidates from their platforms even if those candidates break community guidelines or post illegal, harmful, or hateful content on their profiles. ESICA would not reinvent the wheel, it would destroy it. It would effectively return courts to the dark age of *Stratton Oakmont* liability, obliterate whatever legal distinction remains between the terms "distributor" and "publisher," and force social media companies

[131] Ending Support for Internet Censorship Act, S. 1914, 116th Cong. (2019–2020).

[132] *Id.*

[133] *Id.*

[134] *Id.*

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

to unnecessarily spend millions to simply retain the problematic protection they already receive.

Both the HMA and ESICA strive to adjust Section 230 in accordance with their sponsors' perceived issues with it. However, both bills fail to adequately address the larger issues with Section 230. Although the HMA's language makes some crucial adjustments to clarify Section 230's application, it has no application outside of a national public health emergency. On the other hand, ESICA is a highly partisan response that was drafted to combat the perceived issue of Republican viewpoints getting "shut out" from mainstream social media platforms.[135] This fear is misplaced, and ESICA does nothing to stem the immediate issues with Section 230.

If Congress were to amend Section 230 at all, the legislative response must be not only effective for a variety of national emergencies, but long lasting and flexible enough to cover future technological advancements without completely curtailing incentives for social media companies to continue operating in the United States. Such an amendment might read as follows:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
> (1) Treatment of publisher or speaker
> (A) ***IN GENERAL.—Except as provided in subparagraph (B), no provider*** or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
> (B) ***EXCEPTION.—A provider of an interactive computer service shall be treated as the publisher or speaker of misinformation that is created or developed through the interactive computer service if the provider promotes or develops that misinformation through a non-neutral algorithm used by the provider (or similar software functionality). This subparagraph shall not apply to providers if promotion of misinformation occurs through a neutral mechanism***.

Although the above proposed amendment shares significant similarities with the proposed HMA amendments, it is more broadly applicable to any situation, and it does not require the declaration of a public health emergency or any other type of emergency. This amendment would allow Section 230 to continue to provide general liability protections for social media companies and would simultaneously incentivize all social media platforms to ensure that their algorithms are not

[135] *Senator Hawley Introduces Legislation to Amend Section 230 Immunity for Big Tech Companies*, Josh Hawley: U.S. Senator for Missouri (June 19, 2019), https://www.hawley.senate.gov/senator-hawley-introduces-legislation-amend-section-230-immunity-big-tech-companies.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

promoting or developing misinformation, thus balancing the important interests of public health and safety with free speech in virtual forums. Unfortunately, Congress currently seems powerless to amend Section 230 in a non-partisan way, making it difficult to envision Congress making any productive amendments to it in the coming congressional sessions.

C. Judicial Intervention

But, even if Congress were able to make such an amendment, legislative action is not strictly necessary and would likely create an unneeded influx of litigation over its application. If the problems with Section 230's liability are court-created—and if social media platforms and Congress are unwilling or unable to take effective remedial action—then the Supreme Court must, at long last, interpret the text of Section 230.

Returning to the text as it currently reads, Section 230(c) states:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
>
> (1) Treatment of publisher or speaker
>
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (2) Civil liability
>
> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[136]

[136] 47 U.S.C. § 230(c).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

Strictly construed, Section 230 only protects a provider from being considered the "publisher" of third-party content by neutrally hosting a platform on which that content is posted, i.e., by acting as a "mere conduit" or "neutral distributor."[137] Section 230 also provides immunity for providers that take down or restrict access to objectionable content in good faith.

However, the statute's text does not extend its protections to algorithms that manipulate the information or misinformation that users may see. This interference clearly does not fall within the good faith exception that was meant to fix the perverse *Stratton Oakmont* liability. Justice Thomas said it best: "This modest understanding is a far cry from what has prevailed in court. Adopting the too-common practice of reading extra immunity into statutes where it does not belong, . . . courts have relied on policy and purpose arguments to grant sweeping protection to Internet platforms."[138] In order to address the dissonance between the text of the statute and the lower courts' interpretations of that text, the Supreme Court must return to a strict textual interpretation of Section 230.

Zeran correctly recognized that the internet created "an extraordinary advance in the availability of educational and information resources to [US] citizens," and that "[t]he Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation."[139] To further these objectives, Congress promoted its policy to continue to develop "the Internet and other interactive computer services," and to "preserve the vibrant and competitive free market that presently exists for the Internet . . . unfettered by Federal or State regulation."[140] The CDA was meant to promote self-regulation of the internet, but Section 230 is merely an exception that was meant to immunize providers in very specific situations. For instance, in Section 223(d), Congress criminalized knowingly displaying obscene material to children, even if that material was created by a third party.[141] This directly conflicts with the purpose-driven viewpoint asserted by the Fourth Circuit in *Zeran*—that the CDA was generally meant to immunize providers.

---

[137] *See generally* Enigma Software Grp. v. Malwarebytes, Inc., 946 F.3d 1040 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 13, 15 (2020).

[138] *Id.*

[139] 47 U.S.C. § 230(a).

[140] 47 U.S.C. § 230(b).

[141] 47 U.S.C. § 223(d).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

But there is an even greater danger to maintaining the precedent set by *Zeran*. *Zeran* held that, under Section 230, a service provider is protected from being treated as a publisher or speaker of any information posted by a third party and that, as a matter of law, a service provider is considered a neutral distributor of information unless the plaintiff can show that the provider acted in bad faith.[142] But how can a service provider logically be a "neutral distributor" of information if its algorithms control what information a user is able to view?

There are two primary ways in which the Supreme Court could weigh in on the interpretation of Section 230. First, it could simply affirm the precedent that exists among the circuit courts, permitting an overly broad interpretation of Section 230, and enabling social media companies to receive Section 230's protections even when their algorithms promote detrimental misinformation. This would fortify the overbroad precedent produced by *Zeran* and ultimately fail to protect the public from the dangers of misinformation on the internet during public health emergencies and other national crises.

Alternatively, the Court could overturn, in part, *Klayman v. Zuckerberg* and *Zeran* and strictly construe Section 230. *Klayman* held, among other things, that a social media platform "does not create or develop content when it merely provides a neutral means by which third parties can independently post information online."[143] Instead of qualifying a platform's use of algorithms as neutral distribution, the Supreme Court could interpret non-neutral algorithmic interference with what a user sees in their social media feed as "development of information provided through the Internet" under Section 230(f)(3).

Under this interpretation, Section 230(c)(1) would continue to protect service providers as neutral distributors unless that service provider's algorithms have affected the content shared on the site by another information content provider to the extent that the service provider is no longer a "mere conduit" of that information.[144] By doing so, courts could return the understanding of "publishers" and "distributors" to a pre-*Stratton Oakmont* standard and retain the necessary protections of Section

[142] Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997); *see supra* note 92.

[143] Klayman v. Zuckerberg, 753 F.3d 1354, 1358 (D.C. Cir. 2014).

[144] Malwarebytes, Inc. v. Enigma Software Grp., 141 S. Ct. 13, 14 (2020).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

230, while limiting the protections to those service providers who only act as distributors.[145]

Section 230 is vital to protect free speech on the internet, and it is necessary for social media platforms to continue to flourish in the United States. However, expanding Section 230's protections beyond the text of the statute is unwarranted and provides a blanket exception that ultimately harms the public. In fact, paring back the broad, judicially manufactured liability shield would not open defendants up to intolerable liability; it would merely allow plaintiffs to assert their claims in the first place.[146] Any and all potential plaintiffs would still have to prove their claims. For example, a defamation claim—one of the most common claims a social media platform is likely to face in this context—would still need to reach the exceedingly high bar set by *New York Times v. Sullivan*.[147]

By keeping Section 230 intact—albeit, only to its textual limits—the Court would continue to shield social media sites that moderate their content in good faith and sites that act as mere conduits of information, all while promoting self-regulation, as Section 230 was originally intended to do. However, it would also provide a legal incentive for service providers to use algorithms that neutrally moderate the content posted on their sites—and to do so in good faith. Section 230 would allow plaintiffs to bring their cases when algorithms are non-neutral, thereby encouraging voluntary good faith monitoring of content and more neutral algorithms—perhaps through mechanisms like Meta's Oversight Board—while still protecting social media sites from excessive liability and promoting the free exchange of digital information with a minimum of government regulation.

But most importantly, keeping the construction of the text of Section 230 plain, simple, and clear would allow courts to react to any further technological developments without waiting for congressional action. Adhering to the original text

---

[145] *Id.* at 14 ("Traditionally, [the law] distinguished between publishers or speakers (like newspapers) and distributors (like newsstands and libraries). Publishers or speakers were subjected to a higher standard because they exercised editorial control. They could be strictly liable for transmitting illegal content. But distributors . . . acted as a mere conduit without exercising editorial control, and they often transmitted far more content than they could be expected to review. Distributors were thus liable only when they knew . . . that content was illegal.").

[146] *Id.* at 18 ("Paring back the sweeping immunity courts have read into § 230 would not necessarily render defendants liable for online misconduct. It simply would give plaintiffs a chance to raise their claims in the first place. Plaintiffs still must prove the merits of their cases, and some claims will undoubtedly fail. Moreover, States and the Federal Government are free to update their liability laws to make them more appropriate for an Internet-driven society.").

[147] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

of Section 230 would further permit lower courts to return to the traditional common law understanding of "distributor" and "publisher," creating more consistent precedent that is founded not upon public policy, but upon the law itself.

The Supreme Court had the opportunity to weigh in on this issue this term in *Gonzalez v. Google, LLC* and *Twitter, Inc. v. Taamneh.*[148] These sister cases presented nearly identical issues of fact and law. *Twitter* arose from a 2017 terrorist attack in Istanbul, Turkey, and the plaintiffs sued Facebook, Google, and Twitter under the Justice Against Sponsors of Terrorism Act ("JASTA"), claiming that they aided and abetted ISIS by failing to "detect and remove a substantial number of ISIS-related accounts, posts, and videos" that were crucial to ISIS's organization.[149] *Gonzalez* arose from a 2015 terrorist attack in Paris, France, and the plaintiffs sued Google under JASTA, claiming that Google aided and abetted and conspired with ISIS through Google's video platform, YouTube, by failing to remove ISIS's videos.[150] However, in *Gonzalez*, the Court was directly presented with the question of whether Section 230(c)(1)'s immunization lasts when a service provider makes targeted use of information provided by a separate information content provider.[151]

Petitioners requested that the Supreme Court strictly construe Section 230 to restrict its immunity to traditional editorial functions and to remove any such immunity as applied to non-editorial functions, namely, targeted algorithmic recommendations of information by third parties.[152] Petitioners argued that, because the term "publisher" is derived from defamation law, it has a very narrow meaning that is inapplicable to a provider whose algorithm recommend third-party content, and therefore Section 230's liability shield is entirely inapplicable to algorithmic recommendations.[153] In turn, Respondent argued that a more common understanding

[148] Gonzalez v. Google LLC, 598 U.S. 617 (2023); Twitter, Inc. v. Taamneh, 598 U.S. 471 (2023).

[149] *Taamneh*, 598 U.S. at 482.

[150] *Gonzalez*, 598 U.S. at 621.

[151] *Id.* at 622 ("We granted certiorari to review the Ninth Circuit's application of § 230.").

[152] Brief for Petitioner at 22, 33–34, Gonzalez v. Google, LLC, 598 U.S. 617 (2023).

[153] *Id.* at 19–24.

> The term "publisher" has two meanings. In everyday usage it refers to an entity or person generally engaging in the activity of publishing. . . . But "publisher" (and "publish") has a different meaning in the law, which derives from the law of defamation. A defamatory writing or oral statement is only actionable if the defendant has actually communicated the writing or statement to a person other than the defamed individual. That necessary element of a defamation claim is referred as "publication," and a defendant who in this sense published a

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

of "publisher" is appropriate and, under Section 230, that Petitioners' claims are barred because they attempt to treat Respondent as a "publisher or speaker."[154] Respondent also requested that the Court narrow the focus of the issue presented and avoid "resolv[ing] other amici's alternative arguments that interpret Section 230(c)(1) to foreclose only defamation-like or strict-liability claims," because expanding the Court's decision beyond the bounds of the narrow question Petitioner presented is a real threat to the existence of the internet.[155]

However, Justice Thomas wrote for a unanimous court in *Taamneh*, concluding that the "plaintiffs' allegations are insufficient to establish that [Facebook, Twitter, and Google] aided and abetted ISIS" in carrying out its terrorist attack.[156] As such, although the Court granted certiorari in *Gonzalez* to review the application of Section 230, it was forced to vacate and remand *Gonzalez* because of the Court's disposition in *Taamneh*.[157]

> defamatory statement is referred to as the "publisher" of that statement. "Since the interest protected is that of reputation, it is essential to tort liability for either liable or slander that the defamation be communicated to someone other than the person defamed. This element of communication is given the technical name 'publication. . . .'" "A publication of the defamatory matter is essential to liability. . . . Any act by which the defamatory matter is intentionally or negligently communicated to a third person is a publication."

Id. at 19–20 (internal citations omitted).

[154] Brief of Respondent at 23, Gonzalez v. Google LLC, 598 U.S. 617 (2023) ("Claims that 'treat[]' defendants 'as the publisher or speaker' include those seeking to impose liability for communicating third-party content, including how, whether, and when to communicate it. Here, petitioners' claims treat YouTube as a 'publisher' or 'speaker' because the claims fault YouTube for sorting and displaying, i.e., publishing or speaking, ISIS videos.").

[155] *Id.* at 46; *see also id.* at 33–54.

> Eroding Section 230's protection would create perverse incentives that could both increase removals of legal but controversial speech on some websites and lead other websites to close their eyes to harmful or even illegal content. By proactively or immediately removing any third-party content that anyone might find offensive or objectionable, websites with the resources to find and remove such content (and the advertisers to insist on it) might buy some measure of litigation peace. But it would come at a cost to free expression and access to otherwise legal information. The only third-party content likely to remain would be anodyne, upbeat messaging.

Id. at 53.

[156] Twitter, Inc. v. Taamneh, 598 U.S. 471, 478 (2023).

[157] Gonzalez v. Google LLC, 598 U.S. 617, 621–22 (2023).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

Although the Court recognized during oral argument the significant issues posed by Section 230's interpretations, the Court nevertheless seemed wary to make a significant change to its construction without an understanding how it might impact the tech industry.[158] While it is yet to be seen if, when, and how the Court will interpret Section 230, the Court must seriously consider the implications of failing

> The District Court dismissed plaintiffs' complaint for failure to state a claim, though it offered plaintiffs leave to amend their complaint. Instead, plaintiffs stood on their complaint and appealed, and the Ninth Circuit affirmed in a consolidated opinion that also addressed *Twitter, Inc. v. Taamneh* . . . . With respect to this case, the Ninth Circuit held that most of the plaintiffs' claims were barred by [Section 230]. The sole exceptions were plaintiffs' direct- and secondary-liability claims based on allegations that Google approved ISIS videos for advertisements and then shared proceeds with ISIS through YouTube's revenue sharing system. The Ninth Circuit held that these potential claims were not barred by [Section] 230, but that plaintiffs' allegations failed to state a viable claim in any event.
>
> We granted certiorari to review the Ninth Circuit's application of [Section] 230. Plaintiffs did not seek review of the Ninth Circuit's holdings regarding their revenue-sharing claims. In light of those unchallenged holdings and our disposition of Twitter, on which we also granted certiorari and in which we today reverse the Ninth Circuit's judgment, it has become clear that plaintiffs' complaint—independent of [Section] 230—states little if any claim for relief. As plaintiffs concede, the allegations underlying their secondary-liability claims are materially identical to those at issue in Twitter. Since we hold that the complaint in that case fails to state a claim for aiding and abetting under § 2333(d)(2), it appears to follow that the complaint here likewise fails to state such a claim. And, in discussing plaintiffs' revenue-sharing claims, the Ninth Circuit held that plaintiffs plausibly alleged neither that "Google reached an agreement with ISIS," as required for conspiracy liability, nor that Google's acts were "intended to intimidate or coerce a civilian population, or to influence or affect a government," as required for a direct-liability claim under § 2333(a). Perhaps for that reason, at oral argument, plaintiffs only suggested that they should receive leave to amend their complaint if we were to reverse and remand in *Twitter*.
>
> We need not resolve either the viability of plaintiffs' claims as a whole or whether plaintiffs should receive further leave to amend. Rather, we think it sufficient to acknowledge that much (if not all) of plaintiffs' complaint seems to fail under either our decision in *Twitter* or the Ninth Circuit's unchallenged holdings below. We therefore decline to address the application of [Section] 230 to a complaint that appears to state little, if any, plausible claim for relief. Instead, we vacate the judgment below and remand the case for the Ninth Circuit to consider plaintiffs' complaint in light of our decision in *Twitter*.

Id. (citations omitted).

[158] *See, e.g.*, Transcript of Oral Argument at 45, Gonzalez v. Google LLC, 598 U.S. 617 (2023) ("And, you know, every other industry has to internalize the costs of its conduct. Why is it that the tech industry gets a pass? A little bit unclear. On the other hand, I mean, we're a court. We really don't know about these things. You know, there are not like the nine greatest experts on the Internet.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu

to guide the lower courts in how Section 230 should be read. The Court must orient Section 230's protections in a way that will not only continue to promote freedom of speech on the internet, but correct the questionable precedent left by *Zeran* and protect the public from misinformation during the next national emergency.

CONCLUSION

By expanding Section 230's protections for interactive computer service providers under the guise of legislative purpose, courts have created a foundationless basis for Section 230's sweeping protections. These protections make it impossible for a plaintiff to hold a social media platform liable for health misinformation that could damage the public.

Many advocates argue that Section 230's protections are necessary because it would be impossible for any site to monitor millions of active users. However, continuing to extend protections to non-neutral algorithmic manipulation will allow misinformation to flourish at the expense of public health and safety. Congress could act to change Section 230 to protect the interests of the public, but such action is not necessary, even if Congress is able to develop a reasonable and effective solution to the issue.

Section 230 is not inherently problematic, but its interpretation must be limited to its original text in order to restore its original purpose. The Supreme Court must strictly construe Section 230 so that the impacts of misinformation during the next national emergency can be prevented without sacrificing free speech in cyberspace. Although courts have repeatedly expanded Section 230 by relying heavily upon purpose-driven interpretations of the statute, Section 230's plain meaning appropriately and responsibly outlines the limitations of the exception.

By preserving the textual core of Section 230's exception, the Supreme Court will further Congress's goal to expand free speech with minimum governmental regulation while encouraging responsible self-regulation of algorithms and misinformation by social media companies. However, if the Court fails to act, it will be at the expense of the public, leaving millions of Americans vulnerable to the next destructive wave of misinformation. Although it is too late to stop the detrimental impact of health misinformation during the COVID-19 pandemic, now is the time to preemptively stop the spread of misinformation during the next national emergency by strictly construing Section 230 of the CDA.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.948
http://lawreview.law.pitt.edu