Combating Fake News with "Reasonable Standards"

Tawanna D. Lee
Combating Fake News with “Reasonable Standards”

By TAWANNA D. LEE, M.ED, J.D.*

Abstract

Fake news is an intractable concern around the globe, sowing division and distrust in institutions, and undermining election integrity. This Article analyzes the spectrum of private and public regulation of “fake news” from comparative law and normative perspectives. In the United States, combating fake news shares surprising bipartisan support in an ever-divided political landscape. While several proposals have emerged that would strip Internet media companies of the liability shield for third-party content, it is unlikely that they would survive the seemingly insurmountable First Amendment scrutiny. This Article argues for a different tact—an amendment to the Communications Decency Act that addresses platform design choices rather than speech. In doing so, the Article addresses constitutional concerns of online expression and censorship and demonstrates that a “reasonable standard” is consistent with the existing Internet regulatory framework.

Introduction

In October 2019, Twitter, in addition to other tech platforms and media outlets like YouTube, Facebook, MSNBC, and Fox, ran a 30-second campaign ad that falsely accused Democratic presidential candidate Joe Biden ofblackmailing Ukrainian officials to stop an investigation of his son.1 The viral video was viewed more than 1.5 million times after President Trump posted it to his Twitter account.2 With top performing fake stories

---

like this one reaching users, on average six times faster than content from reputable news outlets.\textsuperscript{3} Internet media companies are powerful vectors for the distribution and amplification of fake news.\textsuperscript{4}

"Fake news" articles have existed for centuries. However, the Internet has enabled them to spread at a rapid pace, with users consuming, processing, and sharing them before anyone has considered their veracity. This phenomenon is particularly pernicious with respect to political information. A 2017 Yale Law School Information Society Project identified that the primary tangible harm that results from fake news is that it "devalues and delegitimizes voices of expertise, authoritative institutions, and the concept of objective data—all of which undermines society’s ability to engage in rational discourse based upon shared facts."\textsuperscript{5} Consider one estimate that suggests that “86% of the groups running paid ads on Facebook in the last six weeks before the 2016 election were suspicious groups, astroturf movement groups,\textsuperscript{6} and questionable news outlets.\textsuperscript{7}

To understand the scale of the problem, consider that a 2019 World Economic Forum Global Risks report continued to call attention to “fake

\begin{quote}

4. Merriam-Webster defines misinformation as “incorrect or misleading information,” whereas disinformation is distinguished as false information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth.” Compare misinformation, Merriam-Webster Dictionary Online, http://www.merriam-webster.com/dictionary/misinformation (last visited Apr. 29, 2020), with disinformation, Merriam-Webster Dictionary Online, http://www.merriam-webster.com/dictionary/disinformation (last visited Apr. 29, 2020). Colloquially, misinformation is understood as merely misleading whereas disinformation is understood as an outright falsehood. As a result, the Article, as do the sources cited, uses the terms interchangeably. Where possible, the article refers simply to “fake news.” It is important to note that “fake news” falls on a spectrum, measured by intent to deceive. The spectrum ranges from satire or parody misleading content on one end of the spectrum, to imposter and fabricated content in the mid-range, followed by false connection, where the imagery, captions, or headlines do not support the content, and false context and manipulated content. See Claire Wardle, Fake News. It’s Complicated, First Draft News (Feb. 16, 2017), https://medium.com/1st-draft/fake-news-its-complicated-d0773766c79.


6. Merriam-Webster defines astroturfing as “organized activity that is intended to create a false impression of a widespread, spontaneously arising, grassroots movement in support of or in opposition to something (such as a political policy) but that is in reality initiated and controlled by a concealed group or organization (such as a corporation).” Astroturfing, Merriam-Webster Dictionary Online, http://www.merriam-webster.com/dictionary/astroturfing (last visited Apr. 29, 2020).

7. Abby K. Wood & Ann M. Ravel, Fool Me Once: Regulating Fake News and Other Online Advertising, 91 S. Cal. L. Rev. 1223, 1230 (2018), https://southerncalifornialawreview.com/wp-content/uploads/2018/10/91_6_1223.pdf. Existing campaign finance laws target paid advertising, which does not reflect the totality of fake news in the Internet media ecosystem. However, as the authors note, there is spending that occurs in various stages of a disinformation campaign, including salary and production that may trigger existing rules.
news” as a leading global risk. This risk assessment reflects a deeper concern that the prevalence of “fake news” has increased political polarization, decreased trust in public institutions, and undermined democracy. These phenomena complicate the means by which our political system operates and the manner in which people hold political leaders accountable. In an Internet media ecosystem, which exposed Americans to more “fake news” than accurate political information during the 2016 U.S. election cycle, the economics of generating clicks and views of sensational or novel headlines over those that are newsworthy underscores the threat to democracy in failing to moderate fake news.

In fact, Internet media companies’ rational self-interest lies in exploiting this phenomenon, increasing advertising revenue by promoting content that drives users to like, click, and share. For instance, during the 2016 election, fake news websites created by profit-driven Macedonian teenagers indicated that the linchpin of their business model was to drive content to social media platforms. While likely not the sole motive for trafficking in “fake news,” the profit margin should not be understated. As a case in point, a New York Times exclusive story about Donald Trump’s purported $916 million loss on his 1995 income tax returns generated a paltry 175,000 Facebook interactions over a month compared to a “fake news” headline from ConservativeState.com, which garnered 480,000 interactions in just one week. But how does the government address the issue of fake news in a manner that does not circumscribe protected speech?

This Article seeks to analyze the spectrum of private and public regulation of disinformation in online political speech, hereinafter referred to as “fake news,” from comparative law and normative perspectives. This Article then proposes an amendment to Section 230 of the Communications

---

8. Id.
14. Id.
Decency Act requiring platforms to adopt “reasonable standards” in order to retain their shield of immunity.

In addressing this issue, Part I will consider the impact of the spread of fake news on the Internet versus fake news consumption of political information via traditional media. Moreover, Part I will review the self-regulatory scheme and its role in the dissemination and amplification of fake news in online political speech. As Part I will illustrate, the tension between industry self-interest and the public interest have necessitated a reexamination of the existing legal framework.

Part II will then provide a comparative overview of the public regulation of online political speech in the European Union and address concerns of censorship and limiting freedom of expression. While many of the legal strategies deployed in the E.U. would be incompatible with the First Amendment, this section will argue that the Internet media companies’ response to these initiatives demonstrate (1) a technological capacity to address “fake speech” in more direct ways than currently exist for the U.S. versions of their platforms; (2) an ability to engage third-party organizations in making determinations about what constitutes “fake news;” and (3) the need for regulation to modify platform behavior to align it in the public interest.

Part III will discuss recent attempts to address the regulation of fake news in online political speech. In particular, this part will consider proposed federal legislation, subsequently enacted state legislation, and resulting the judicial determinations about the constitutionality of attempts to regulate political speech.

Finally, Part IV offers a recommendation to apply a legislative framework tailored for the Internet ecosystem that would provide guard rails against political “fake news” while respecting constitutional limitations on regulating speech. Specifically, the Article proposes an amendment to Section 230 of the Communications Decency Act, by carving out “reasonable standards” safe harbors under which Internet media companies may maintain the statutory immunity they enjoy for content posted by third parties.

Current State of Online Political Speech in the U.S.

Self-Interest and Self-Regulation Come to a Head in the Face of “Fake News”

What is fake news? NPR political reporter, Danielle Kurtzleben, notes that while contemporary political figures have co-opted the term “fake news” to devalue unfavorable news, fake news has traditionally referred to “lies
posing as news.”\textsuperscript{15}  Fake news, in the traditional sense, is “a media product fabricated and disguised to look like credible news that is posted online and circulated via social media.”\textsuperscript{16}  Either of these “strategic uses of “fake news”—to achieve specific political results and to destabilize the press as an institution—are self-evidently very dangerous for democracy.”\textsuperscript{17}

Traditional media arguably “expose[s] people to a range of topics and views at the same time that they provide shared experiences for a heterogeneous public.”\textsuperscript{18}  Conversely, Internet media companies provide platforms that leverage technology to “infiltrate a population of unaware humans and manipulate them to affect their perception of reality, with unpredictable results.”\textsuperscript{19}  “[F]actual knowledge about politics is a critical component of citizenship, one that is essential if citizens are to discern their real interests. . . . In the absence of adequate information neither passion nor reason is likely to lead to decisions that reflect the real interests of the public.”\textsuperscript{20}  The erosion of public trust in traditional news sources creates a vacuum filled by misinformation.  Regulating “fake news” in online political speech in the context of an election is critical to protecting the rationality of electoral outcomes.

As researchers Alice Marwick and Rebecca Lewis note, the spread of misinformation leads to decreased trust in media, the impact of which “weaken[s] the political knowledge of citizens, inhibits its watchdog function, and may impede the full exercise of democracy.”\textsuperscript{21}  This phenomenon is exacerbated by social and political divisions that undermine the traditional ways in which truth ordinarily prevails. “Investigations, exposés, and studies fall short in a situation where a significant portion of the population distrusts a wide array of sources they perceive as politically or ideologically hostile


\textsuperscript{16}  Nina I. Brown & Jonathan Peters, \textit{Say This, Not That: Government Regulation and Control of Social Media}, 68 SYRACUSE L. REV. 521, 521-22 (2018), https://heinonline.org/HOL/P?h=hein.journals/syrlr68&i=557.  Notably, this definition excludes unintentional reporting mistakes, conspiracy theories, satire that is unlikely to be misconstrued as factual, false statements by politicians, and reports that are slanted but not outright false.


\textsuperscript{18}  Cass R. Sunstein, \textit{The Republic: Divided Democracy in the Age of Social Media} 43 (2018).

\textsuperscript{19}  West, \textit{supra} note 9.


\textsuperscript{21}  Marwick, \textit{supra} note 11 at 45.
Constitutional Protection

The First Amendment and the Communications Decency Act stand as bulwarks to regulating online political speech. The First Amendment provides that “Congress shall make no law . . . abridging the freedom of speech; or the press.” Moreover, “the First Amendment has its fullest and most urgent application to speech uttered during a campaign for political office.” The online dissemination of political opinions and information are incontrovertibly political speech and is therefore protected by the First Amendment. Under the strong protections afforded to political speech, several legislative attempts to regulate in this space have been defeated. For example, in Washington Post v. McManus, 944 F.3d 503 (4th Cir. 2019), the court found

The lodestar for the First Amendment is the preservation of the marketplace of ideas. When the government seeks to favor or disfavor [political speech] . . . it compromises the integrity of our national discourse and risks bringing about a form of soft censorship. For this reason, content-based laws are “presumptively unconstitutional,” the presumption being necessary to ensure that the marketplace of ideas does not deteriorate into a forum for the subjects of state-favored speech. . . . Because our democracy relies on free debate as the vehicle of dispute and the engine of electoral change, political speech occupies a distinctive place in First Amendment law.

Regulation of political speech “trenches upon an area in which the importance of First Amendment protections is at its zenith.” Buttressing such strong protections of political speech—and hampering regulation on

23. U.S. CONST. amend. I.
25. See id. at 510 (invalidating Maryland’s SB875, Online Electioneering Transparency and Accountability Act).
26. Id.
27. Id. at 514 (quoting Meyer v. Grant, 486 U.S. 414, 425 (1988)) (internal quotations omitted).
“fake news”—the Supreme Court, in a plurality opinion, extended full free speech protection to a knowing and intentional falsehood. While content-based laws—those that “target speech based on its communicative content . . . may be justified only if the government proves that they are narrowly tailored to serve compelling state interests,” the Court has recognized a compelling interest in maintaining the integrity of the electoral process; however, it has stopped short of extending that to preventing fraud on the electorate. Absent reliable data demonstrating that false speech has significantly undermined the electoral process, however, it is unlikely that a court would find that this prong had been satisfied. Notwithstanding the difficulty in demonstrating significant harm, it is dubious that compelling Internet media companies to curb fake news is the least restrictive means of achieving that interest.

Federal Legislation

The Communications Decency Act (“CDA”), referred to in the industry simply as Section 230, was borne from concerns of defamation and indecency liability to address “the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium.” Touted as “the law that gave us modern Internet,” Section 230 provides statutory immunity to online platforms from treatment as a publisher or speaker. The argument for this shield was a recognition that if Internet media companies could be liable for all user-generated content that they moderated, they wouldn’t moderate anything at all.

28. U.S. v. Alvarez, 567 U.S. 709, 721-22 (2012) (“This opinion . . . . rejects the notion that false speech should be in a general category that is presumptively unprotected.”). In Alvarez, the false speech at issue was Alvarez’s misrepresentation that he had won the Congressional Medal of Honor.
31. 129 F.3d 327, 328, 330 (4th Cir. 1997). While the indecency prong was held unconstitutional by the Supreme Court, the defamation prong has become a lynchpin of the Internet ecosystem. Reno v. ACLU, 521 U.S. 844, 874 (1997) (striking down indecency prong).
Following judicial decisions holding online providers liable for user content.34 In Zeran v. America Online, the court opined that the specter of strict liability normally applied to publishers might chill the free flow of information.35 In response, it offered protection for “good Samaritan” blocking and screening of offensive material to encourage service providers to self-regulate the dissemination of offensive material over their services.36 As Senator Ron Wyden, a drafter of the CDA, notes, this ensured “that companies in return for that protection—that they wouldn’t be sued indiscriminately—were being responsible in terms of policing their platforms.”37

Specifically, Section 230 provides that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”38 An interactive service provider is defined as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server.”39 This shield extends to Internet media companies the relief that their offline counterparts—bookstores, newsstands, libraries, and other “distributors”—receive under common law.40

However, broad judicial interpretation of Section 230 has provided immunity for conduct far beyond, and likely in direct conflict with, that which was contemplated by the CDA’s drafters who wanted to incentivize platforms to clean up the Internet.41 As Professor Tushnet opines, “[o]ne way to explain §230 is that it was enacted in the hope that ISPs would shut down speech that Congress couldn’t constitutionally ban. From this perspective, § 230 largely backfired.”42 Section 230 has offered platforms

34.  See e.g., Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (holding that the defendant’s message board was akin to a newspaper, and as such, by taking steps to police the content of this message board, the defendant engaged in an editorial function that exposed it to publisher liability).
35.  Zeran, 129 F.3d 327 at 330 (“the amount of information communicated via interactive computer services is . . . staggering. The specter of tort liability in an area of such prolific speech would have an obviously chilling effect.”).
41.  Selukh, supra note 37.
“power without responsibility,”43 shielding sites that host revenge porn,44 child predation,45 housing discrimination,46 and online sex trafficking.47

Internet Media Companies are the Appropriate Vehicles for Regulation

As a result of these two forces, Internet media companies rely on self-regulatory exercises to address “fake news” with respect to political speech. Notwithstanding a shield of immunity against liability for third-party content, Internet media companies engage in a great deal of moderation—shadow banning, blocking, filtering—when it proves bad for business.48 The lack of government regulation in this space has resulted in a patchwork of content moderation practices that has garnered the attention—and frustration—of federal legislators.49

Coordinated regulation is the appropriate response to the evolving media landscape wherein exists a conflict of self-interest, and where political vulnerability renders the current self-regulatory approach inapt.50 Cooperation between public and private entities is a necessary part of 21st century Internet regulation. Internet media companies are best positioned to mitigate harm because of their expertise on the issues that arise on their platforms and the technical requirements necessary to address them, whereas government regulation is required to provide accountability and an enforcement mechanism.51 Government coordination provides several important functions, including coordination facilitation, signaling to actors, behavior modification, and value setting.52

43. Id.
46. See e.g., Chicago Lawyers’ Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008); Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).
47. See e.g., Dart v. Craigslist, Inc., 665 F. Supp. 2d 961 (N.D. Ill. 2009). Recognizing that judicial interpretation had stretched liability protection beyond its original intent, Congress cabined Section 230’s immunity with the passage of the Stop Enabling Sex Traffickers Act (SESTA)/ Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) legislation. The controversial amendment provided a carve out in immunity from federal civil and state criminal liability for services that “promote and facilitate prostitution.”
48. See e.g., DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE, 229 (2014) (discussing how Facebook changed its position on pro rape pages after fifteen companies threatened to pull their ads).
50. Wood, supra note 7.
51. Wood, supra note 7.
52. Id at 1244.
Technology companies, including Facebook, have signaled their support for modernizing the law to hold Internet media companies accountable for behavior on their platforms and more recently the platforms have been more amenable to a new regulatory framework.

The U.S. Regulatory Scheme: Industry Self-Regulation of “Fake News” in Online Political Speech

Benefits of Self-Regulation

According to proponents, “the benefits of industry self-regulation are apparent: speed, flexibility, sensitivity to market circumstances and lower costs.” Moreover, when standard setting is executed by industry insiders with deep subject-matter expertise, the resulting standards are arguably more practicable and more effectively policed. Proponents also maintain that industry accountability raises standards of behavior through a combination of peer pressure and an internalized sense of responsibility. This elevated standard of behavior is perhaps evident in the Internet Media companies’ response to the global pandemic of COVID-19.

It is notable, however, that the Internet media ecosystem appears divorced from a typical industry self-regulation model wherein there is “an industry-level organization that regulates its members by setting rules and standards about how they should conduct their business.” Instead, individual companies have scrambled to provide the appropriate regulatory scaffolding—and stave off regulation.

53. See Mark Zuckerberg, Mark Zuckerberg: The Internet needs new rules. Let’s start in these four areas, WASH. POST (Mar. 30, 2019, 3:00 p.m. EDT), (“I believe we need a more active role for governments and regulators. By updating the rules for the Internet, we can preserve what’s best about it—the freedom for people to express themselves and for entrepreneurs to build new things—while also protecting society from broader harms.”), https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.htm.


56. See id.

57. Internet media companies quickly developed strategies to provide their users with authoritative information on the virus, employed tools to combat misinformation, and provided data for research. See e.g., Jonathan Shieber, Zuckerberg details the ways Facebook and Chan Zuckerberg Initiative are responding to COVID-19, TECHCRUNCH (Mar. 3, 2020, 8:20 PM PST), https://techcrunch.com/2020/03/03/zuckerberg-details-the-ways-facebook-and-chan-zuckerberg-initiative-are-responding-to-covid-19/.

58. Wood, supra note 7.
The Dark Side of Self-Regulation

In practice, self-regulation often faces backlash for its perceived self-interested behavior. Cynics decry self-regulation as a façade by which industry “give[s] the appearance of regulation thereby warding off more direct and effective government intervention while serving private interests at the expense of the public.”59

Critics admonish that self-regulatory standards are usually lax and enforcement is ineffective.60 Detractors also note that absent from self-regulation are many of the virtues of conventional public regulation, namely, “visibility, credibility, accountability, compulsory application to all[,] . . . greater likelihood of rigorous standards being developed, cost spreading, . . . and availability of a range of sanctions.”61

Left to their own devices, concern has arisen that content moderation strategies adopted by Internet media companies may not comport with customary First Amendment norms and doctrine. As legal scholars highlight, Internet media companies “lack a coherent theory of the First Amendment.”62 Platforms are not “merely venues for debates in the marketplace of ideas,” neither are they “exclusively supportive of speakers’ personal autonomy,” nor have they “taken a [] deliberation-enhancing approach to speech . . . [that] should promote political engagement and public discourse.”63 Instead, the largest players in the Internet media landscape have camped out in their respective corners, leaving the field an “inconsistent amalgam” of these values.64

Writ large, there is reason to be concerned with putting speech regulation wholly in the hands of private corporations. As Verge tech reporter Casey Newton points out, “[i]f you don’t want the state making calls on political speech, you probably don’t want a quasi-state with 2.1 billion daily users making calls on political speech, either.”65

U.S. Social Media Self-Regulation—Case Study: Drunk Nancy Pelosi

A recent fake news story circulating in U.S. news aptly illustrates the dissemination and amplification of fake news at a scale impossible via

---

59. Gunningham, supra note 55 at 369-70.
60. See id. at 370.
61. Id.
63. Id.
64. Id.
traditional media. The online sphere is the critical factor because of the speed, anonymity, and volume of content it allows. On Wednesday, May 23, 2019, an altered video that made it appear that House Speaker Nancy Pelosi was drunk began to circulate broadly across social media platforms.\textsuperscript{66} On Thursday evening, following a Fox Business news segment in which panelists speculated about the House Speaker’s health and fitness for office, President Donald Trump himself tweeted and then pinned to his profile another manipulated video of the House Speaker to his estimated 60 million Twitter followers.\textsuperscript{67} The altered video with the caption, “PELOSI STAMMERS THROUGH NEWS CONFERENCE” was slowed down to make her voice sound sluggish and her words appear slurred.\textsuperscript{68} The combination of the two videos and speculation about the Speaker’s health quickly gained attention. National media outlets immediately published critical responses about the particular brand of misinformation at play, a “shallow fake,” and called for Internet media companies to take action.\textsuperscript{69}

The incident illustrates not only the role that online media companies can play in amplifying “fake news” but the way in which such “fake news” can make its way into mainstream news discourse. Internet media companies engage in varying degrees of regulating online political speech through their community standards and terms of service. Google’s YouTube took swift action to remove the video.\textsuperscript{70} However, Facebook’s community standards do not require that information posted on the platform is true.\textsuperscript{71} Instead, its policy at the time that the video was posted was to refer it to third-party fact checkers for review.\textsuperscript{72} The third-party fact checkers rated the video as false, and in accordance with the social media platform’s policy, downgraded the video’s distribution and provided additional context where it appeared in


\textsuperscript{68} Id.

\textsuperscript{69} “Shallow fake” is a term used to describe the traditional-alteration and selective editing of video and imagery. See Kalev Leetaru, The Real Danger Today is Shallow Fakes and Selective Editing Not Deep Fakes, FORBES (Aug. 26, 2019, 1:11 PM EDT), https://www.forbes.com/sites/kalevleetaru/2019/08/26/the-real-danger-today-is-shallow-fakes-and-selective-editing-not-deep-fakes/#607caee1f4e0.


\textsuperscript{71} Id.

\textsuperscript{72} Id.
users’ news feeds. Nonetheless, one version of the video had 2.5 million views on its platform in just 12 hours after the video was posted.

Internet Media Companies’ Varied Approaches to Self-Regulation in the U.S.

On one end of the spectrum, Twitter announced an outright ban on political advertising on its platform. Twitter CEO, Jack Dorsey recognizes the shift that the Internet presents in the ways that political information is consumed. Dorsey explained in a tweet that “Internet political ads present entirely new challenges to civic discourse—machine-learning-based optimization of messaging and microtargeting, unchecked misleading information and deep fakes, all at increasing velocity, sophistication and overwhelming scale.” Though the move was largely viewed as symbolic, it sets the social media platform apart in the Internet media ecosystem. With digital advertising costing a fraction of traditional television advertising, observers decry the move as disadvantaging challengers while supporting entrenched candidates. In May 2020, Twitter took further action and began applying a new label to tweets that contain potentially misleading information about voting processes. For example, a new label prompting Twitter users to “Get the facts about mail-in ballots” accompanied a set of tweets in which the president railed against mail-in voting methods as “fraudulent.”

Following Twitter’s announcement of its ban on political advertisements, Google, announced an update to its political advertising policy, with the goals to “protect campaigns, surface authoritative election

---

73. Id.
74. Id.
77. It should be noted that Twitter’s political advertising comprised a small fraction of its advertising business. Moreover, the free exposure that the platform provides politicians more than accounts for any loss in advertising opportunity. For example, according to The Guardian’s Shannon McGregor, 80% of President Trump’s tweets make their way into mainstream media, garnering media exposure. That exposure was valued at an estimated $2bn during the 2016 election cycle. See generally Shannon C. McGregor, Why Twitter’s Ban on Political Ads Isn’t As Good As it Sounds, THE GUARDIAN (Nov. 4, 2019, 6:00 EST), https://www.theguardian.com/commentisfree/2019/nov/04/twitter-political-ads-ban.
78. McGregor, supra, note 76.
news, and protect elections from foreign interference.” 81 Attempting to align itself with traditional media outlets, such as TV, radio, and print, Google has prohibited political campaigns from engaging in microtargeting, an advertising technique that uses consumer data, online behavior, and demographics to tailor messaging. 82 Microtargeting has been viewed as “the online equivalent of whispering millions of different messages into zillions of different ears for maximum effect and with minimum scrutiny.” 83 In particular, political campaigns are no longer permitted to target “affinity audiences” or “remarket”—serve ads to people who’ve previously taken an action, for instance visiting a campaign’s website. 84 Striking at the heart of the problem of fake news, advertisements with “demonstrably false claims that could significantly undermine participation or trust” in elections are now banned. 85

On the other end of the spectrum, Facebook has made the controversial decision to continue to allow political “fake news” to propagate across its platform. Instead, Facebook’s policy is merely to provide additional context, by way of “related news” links appearing next to “fake news.” By late July 2020 pressure on Internet media companies to label potentially misleading information led Facebook to adopt what critics decry as a half-measure. The platform implemented a new policy to add a link to official voting information to any post about voting, whether the post is John Q. Citizen or a political candidate and regardless of whether the content is accurate. 86 Facebook’s stance on not fact checking advertisements from politicians can be explained, at least in part, by what Professor Philip Napoli identifies as “a First Amendment tradition that has valorized the notion of counter[s]peech.” 87

Facebook’s community standards prohibit “misinformation” defined as “ads that include claims debunked by third-party fact checkers or, in certain circumstances, claims debunked by organizations with particular

84. Id.
85. Spencer, supra, note 81.
87. Philip M. Napoli, What If More Speech Is No Longer the Solution? First Amendment Theory Meets Fake News and the Filter Bubble, 70 FED. COMM. L.J. 55, 58 (2018) (internal quotations omitted); see e.g., Alvarez, 567 U.S. at 727 (“The remedy for speech that is false is speech that is true.”).
expertise.” While paid political advertising must conform to the platform’s community standards, Facebook VP of Global Affairs and Communications, Nick Clegg, clarified that most political advertisements would be exempt from the platform’s fact-checking. The platform has not addressed the hot-button issue of microtargeting. Political strategists highlight Facebook’s desire to walk the fine line between moderating content and alienating groups who leverage the platform’s access to an estimated 70% of American adults in their campaign fundraising efforts.

Facebook’s practices allow it to adopt an approach that, on the one hand, espouses transparency whereby political advertisements are available to the public so that researchers, journalists, and John Q. Citizen can investigate the content of those ads themselves, while on the other hand continuing to advance a business model predicated on generating advertising revenue by exerting near-total control of users’ online experience.

Legislators have cautioned that Internet media companies are abusing the immunity extended to them by the Communications Decency Act. Some have indicated that removal of such immunity is not out of the question, and were Congress to act, it would end the self-regulation regime in the U.S., moving things more in line with the E.U. model.

Current State of Online Political Speech in the E.U.

The model for combating fake news in the European Union stands in direct contrast to the self-regulatory framework of the U.S. Europe has traditionally favored regulation over freedom of expression. Identifying fake news as a “threat to democratic political and policy-making processes,” the European Union has adopted a public governance approach combating it. While incompatible with the First Amendment, a comparative overview of

89. Facebook, Elections and Political Speech, FACEBOOK: NEWSROOM (Sept. 24, 2019, https://about.fb.com/news/2019/09/elections-and-political-speech/ (“We don’t believe [] that it’s an appropriate role for us to referee political debates and prevent a politician’s speech from reaching its audience and being subject to public debate and scrutiny.”)).
93. Id.
public regulation of online political speech in the European Union highlights three phenomena: (1) a technological capacity to address “fake speech” in more direct ways, (2) a workable framework for engaging third-party organizations so as to avoid being “arbiters of truth,” and (3) the need for regulation to modify platform behavior for the public good.

Since 2015, following a decision of the European Counsel in response to Russian disinformation campaigns, the E.U. has been actively regulating disinformation,\(^4\) defined as “verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public.”\(^5\) In 2018, the European Commission took additional steps to crack down on “fake news,” adopting The Action Plan against Disinformation (“The Plan”).\(^6\) The first prong of The Plan focuses on improving detection of disinformation, through investment in additional staff, data analysis tools, and public education efforts.\(^7\) In the second prong of the plan, the E.U. implemented a coordinated alert system among E.U. institutions and member states to respond to disinformation threats in real time.\(^8\) With respect to U.S. efforts, the third prong of the approach is noteworthy. The third prong of the approach included the adoption of a self-regulatory Code of Practice on Disinformation as a component of its Action Plan against Disinformation. Among seven European trade associations, U.S. signatories to the Code of Practice include Internet media companies Facebook, Google, Microsoft, Mozilla, and Twitter.\(^9\) The Code of Practice seeks to ensure transparency in political advertising, the shuttering of fake accounts, identifying non-human interactions, and cooperating with fact-checkers to detect disinformation and widely promote fact-checked content.\(^10\) Each signatory presented detailed roadmaps highlighting the tools to be deployed against fake news.\(^11\)

---

7. Id.
9. Id.
10. Id.
E.U. Public Regulation of Fake News in Online Political Speech

Transparency, accountability, and consumer protection are often touted benefits of public regulation. Detractors argue that federal regulation may be excessively burdensome. Researchers point to three phenomena that undermine the utility of public regulation. “First, agencies intermittently overreact to crises, and years, if not decades, may pass before guidelines developed in the aftermath of crises are corrected. Second, government agencies are not liable for inefficient rules, undermining the financial accountability necessary to incentivize efficient rulemaking and thereby potentially promoting over-regulation.” 102 The pace of industry transition exacerbates the shortcomings of general agency regulation with rapid technological evolution outpacing government regulation. This is evident in the conversation on the Hill with respect to modernizing the twenty-four year old Communications Decency Act that was penned almost a decade before Facebook was founded.

Other detractors condemn government regulation as exceedingly flexible and under-enforced for a myriad of reasons: lack of resources, insular perspectives of government, self-serving administrators, or regulatory capture.103 Moreover, changes between administrations may lead to vacillation between standards. 104 The revolving door between political appointments and private sector executive suites may also foster a climate whereby administrators may seek to improve their prospects in industry by advancing the agenda of interest groups that desire loose policies.105

E.U Social Media Public Regulation – Case Study: Maria and the Mafia

In November 2017, in the weeks before Italy’s national election, photographs began to circulate that purported to show Maria Elena Boschi, a prominent lawmaker and member of former Prime Minister Matteo Renzi’s ruling Democratic Party, at a funeral mourning the recent death of the notorious mafia boss Salvatore “Toto” Riina. 106 The doctored picture included a caption: “Look who was there to say one last goodbye to Toto Riina?”107 The photo, shared by a Facebook account with a profile image which appeared to attribute the post to opposition political party, 5 Star

---

103. Id. at 568–69.
104. Id.
105. Id.
Movement (Virus5Steele) is real—taken at a 2016 funeral of a Nigerian refugee who was murdered. The account was later determined to a fake.108

Without a disinformation policy in place, the Italian government was dependent on Facebook to police the fake news. “We ask the social networks, and especially Facebook, to help us have a clean electoral campaign,” said Mr. Renzi.109 Boschi herself took to Facebook to decry the fake news with the hashtag #nofakenews.110 Following pleas of help from the Italian government, Facebook announced a fact-checking program similar to the U.S. program that relies on third-party fact checkers and user reporting aimed at identifying and debunking false information. The program works with third-party fact-checking organizations to develop additional fact-checking reporting which is then posted prominently near the false story and subsequently demoted on the Facebook algorithm.111 Unlike the U.S. program, when a user attempts to share the fake news, a notification alerts them of the disputed content and refers them to additional information.112 The Italian government has dedicated resources to educate its citizenry on detecting fake news.113 This situation demonstrates the vulnerability of the political process to come under attack by unknown perpetrators and the facility with which Internet media companies can take reasonable steps to combat fake news.

Italy’s antitrust chief enforcer, Giovanni Pitruzella argued that the distribution of fake news violates European citizen’s “right to be pluralistically informed.”114 Moreover, he urged the government to get involved in verifying information and the removal of “fake news” to avoid “group polarization.”115 As Justice Kennedy cautioned in United States v. Alvarez, the government serving as arbiter of what is fake is simply untenable in the United States as incompatible with the First Amendment. In his words,

108. Id.
110. Jiménez, supra, note 106.
112. Id.
113. Id.
115. Id.
[p]ermitting the government to decree [false] speech to be a criminal offense . . . would endorse government authority to compile a list of subjects about which false statements are punishable. . . . Our constitutional tradition stands against the idea that we need Oceania’s Ministry of Truth.116

Other European countries have taken definitive steps to legislate fake news. In 2017, the German Bundestag passed the Network Enforcement Act, an “Act to Improve Enforcement of the Law in Social Networks” (“NetzDG”), a law that requires Internet media companies with greater than two million registered users to block and delete illegal content, while increasing transparency and accountability of platform content removals, subject to monetary fines up to €5 million for noncompliance.117 Notably, NetzDG mandates that platforms “remove[,] or block[,] access to content that is manifestly unlawful within 24 hours of receiving the complaint.”118

The law has come under fire, in relevant part with respect to “fake news,” because it provides that “the decision regarding the unlawfulness of the content is dependent on the falsity,” which is determined by the platforms themselves.119 Volker Tripp, political director of the non-profit internet rights organization Digitale Gesellschaft (“digital society”) noted that “unilaterally shifting this responsibility onto companies is legally questionable and on top of that not productive.”120 Though Facebook ran afoul of NetzDG for allegedly underreporting the complaints that the platform received,121 critics assert that the law incentivizes companies to “delete in doubt” because it compels decision-making within such a short time period.122

118. Id.
119. Id.
Internet Media Companies’ Response to Public Regulation

In response to the German law, each of the “Big Three” online media companies, Google, Facebook, and Twitter, took differing compliance approaches. Google and Twitter developed an integrated NetzDG flagging tool whereby users can directly report objectionable content. In contrast, Facebook has embedded its NetzDG complaint form in its Help Center. Facebook’s dedicated team first reviews reported content for compliance with Facebook’s community standards. Content found in violation of the platform’s community standards are removed globally. If the content is violative of NetzDG but does not run afoul of the community standards, the content is blocked in Germany and reported. This two-step review process and the obscured location may be attributable to the relatively lower reporting rates discussed above.

Twitter has likewise assembled a compliance team of 50 staff specifically designed to address NetzDG complaints according to the NetzDG’s narrower definition of illegal content. Elsewhere, content is first reviewed according to Twitter’s terms and conditions. Google’s team removes most content for violating community guidelines, rather than NetzDG noting that the two “have a large degree of overlap.” While the platforms handle most takedowns internally, both Facebook and Google work in collaboration with a voluntary intermediary to review questionable content within the mandated 7-day timeframe.

Testing the Regulatory Boundaries of Online Political Speech in the U.S.

Under the existing jurisprudential framework, the United States government appears relegated to taking no more than small steps to combat fake news. The United States government frequently requests that Internet

---

124. Id.
125. Id. at 8.
126. Id.
127. Id. at 11.
128. Id.
129. Id. at 10.
130. Id. at 12.
131. First Amendment protections limit the government’s ability to regulate political speech; however, other federal national security and campaign finance laws compel transparency and disclosure. See 52 U.S.C. §30121 (2012) (discussing contributions and donations by foreign
media companies remove content or delete user accounts that the government finds problematic. Such requests go unanswered. A number of federal legislative proposals have been advanced to update the government’s toolbox in its battle against “fake news.”

The Honest Ads Act

Spurred in part by allegations of attempted election interference by Russian nationals, in October 2017, Senators Amy Klobuchar (D-MN), Mark Warner (D-VA), and the late Senator John McCain (R-AZ) introduced the Honest Ads Act, which would extend existing campaign finance regulations for broadcast advertising to online platforms. The Honest Ads Act would subject Internet media companies to transparency and record-keeping requirements. The bill stalled; however, it was reintroduced in May 2019, again with bipartisan co-sponsorship and bolstered by industry support.

The Online Electioneering Transparency and Accountability Act

States have also entered the battle to protect the integrity of the nation’s electoral process. The Maryland law, SB 875, the Online Electioneering Transparency and Accountability Act, took effect in July 2018. Drawing from language in the Honest Ads Act, the law extended Maryland’s existing campaign finance regulation law governing traditional media in two critical ways with an eye toward the Internet domain. First, the new law added online advertisements to the record-keeping and disclosure requirements. Specifically, the record-keeping and disclosure provision required online platforms to disclose the identity of an ad purchaser, the individuals who

---


133. Id. (Of the 170 removal requests made on behalf of the U.S. government between January and June 2019, identifying 732 accounts, Twitter complied with zero requests).

134. The rules, which also banned foreign nationals from paying for ads that mention political candidates leading up to elections, are outlined in the Bipartisan Campaign Reform Act (BCRA) of 2002, also known as McCain-Feingold, which laid out the requirements for “electioneering communications” in broadcast, cable, and satellite communications. Bipartisan Campaign Reform Act, Pub. L. 107-155, 116 Stat. 81 (2002).

135. Honest Ads Act, S. 1989, 115th Cong. (2017). The Bipartisan Campaign Reform Act (BCRA) of 2002, also known as McCain-Feingold, which laid out the requirements for “electioneering communications” in broadcast, cable, and satellite communications, served as a blueprint for the bill. The Honest Ads Act also banned foreign nationals from paying for ads that mention political candidates leading up to elections.

exercise control over the purchaser, and the total amount paid for the ad. This information was required to be maintained for inspection for up to a year following an election. Second, the state extended its reach to “online platforms,” defined as “any public facing website . . . including a social media network or search engine that has 100,000 or more . . . visitors.”

Publishers, including The Washington Post and The Baltimore Sun, challenged the new law on First Amendment grounds because the disclosure requirements compelled the publishers to engage in speech. The Fourth Circuit sitting en banc affirmed a federal district court’s decision to enjoin enforcement of the record-keeping and disclosure requirements, raising several First Amendment grounds: (1) the Act is an impermissible content-based regulation on speech; (2) “the Act concerns content that is ordinarily shielded within “the heart of the First Amendment’s protection,” and (3) the Act compels speech. “In sum, it is apparent that Maryland’s law creates a constitutional infirmity distinct from garden-variety campaign finance regulations.”

Notwithstanding the bipartisan support that the Honest Ads Act garnered and the passage of the state legislation, both efforts are ill-suited to address “fake news” because their focus on paid advertising overlooks the volume of Internet-enabled “cheap speech.” The economic implications of potentially anyone disseminating speech “have undermined mediating and stabilizing institutions of American democracy including newspapers and political parties, with negative social and political consequences.”

Proposed Executive Order

The assault on fake news in the United States reached a fever pitch on May 28, 2020, as President Trump released an Executive Order that takes aim at the intermediary liability protections that Section 230 extends to Internet media companies. The Executive Order appears to be a reboot of a 2017 draft that received renewed attention from the administration after two of the President’s tweets on mail-in voter fraud were flagged as misleading. Striking at the heart of Communications Decency Act,
Section 230, the Executive Order calls for government review of Internet media companies’ content moderation practices, declaring that “[w]e must seek transparency and accountability from online platforms, and encourage standards and tools to protect and preserve the integrity and openness of American discourse and freedom of expression.”

The Executive Order, “Preventing Online Censorship,” addresses perceived bias by Internet media companies in moderating political speech. The White House seeks to curtail the good-faith provision of the Communications Decency Act by imposing additional obligations on Internet media companies seeking liability protections. Specifically, the Executive Order attempts to tie the “good faith” liability shield in Section 230(c)(2), which immunizes platforms from liability arising from “any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene . . . or otherwise objectionable,” to the protections in Section 230(c)(1), which protects platforms from being treated as speakers. The Executive Order invokes sweeping government action to regulate Internet media companies. Among other actions, the order directs the National Telecommunications and Information Administration to file a petition for rulemaking with the Federal Communications Commission to “propose regulations to clarify” the scope of Section 230, directs the Federal Trade Commission to report on complaints of political bias, instructs the Department of Justice to investigate allegations of anti-conservative bias, and prevents federal agencies from advertising on platforms that allegedly violate Section 230’s good faith principles. Notwithstanding the jurisdictional and constitutional concerns that it raises, the Executive Order demonstrates a political openness to stipulate safe harbors for Internet media companies to retain liability protection.


144. Executive Order, supra, note 142.


146. Id.

147. Id.
Proposed Model: Coordinated Regulation through “Reasonable Standards”

The growing political will in both the legislative and executive branches to revisit the regulation of Internet media companies represents a moment to exercise reasonableness in addressing the 26 words that created the Internet. A coordinated regulatory approach would capitalize on the strengths and virtues of industry self-regulation, while accounting for its weaknesses as a self-interested body.

Professors Danielle Citron and Benjamin Wittes advance a proposition that conditions immunity not on a platform’s content moderation, but rather on the platform’s design choices. This “precision regulation” approach would strip immunity for Internet media companies whose “design choices [ ]amounted to a failure to take reasonable steps to prevent or address unlawful uses of its services.”148 What is more, observers have noted that the harms resulting from “fake news” are less about what is shared, rather than how it is shared.149 After all, the Internet has revolutionized the speed and volume with which fake news is propagated. What users see is determined entirely by the algorithms deployed by Internet media companies that rank and prioritize content. “They design and predict nearly everything that happens on their site, from the moment a user signs in to the moment she logs out.”150

The proposed amendment to Section 230(c)(1) reads, in relevant part, that

[n]o provider or user of an interactive computer service that takes reasonable steps to prevent or address unlawful uses of its services shall be treated as the publisher or speaker of any information provided by another information content provider in any action arising out of the publication of content provided by that information content provider.151

149. See e.g., The Information Society Project, supra note 5 at 5.
151. Citron, supra, note 147 at 419.
Under this conceptualization, adopting a reasonable standard of care replaces the broad immunity currently enjoyed with an affirmative defense against liability claims. As Citron notes, the reasonable standard would examine whether the company employed reasonable content management practices writ-large, rather than with respect to a particular use of the service. As such, the reasonableness standard offers flexibility to evolve as the existent technology does.

Some have balked at reforming Section 230, warning that it would stifle innovation and end the Internet as we know it. Critics are also wont to cite Congress’ desire to “encourage the unfettered and unregulated development of free speech on the Internet.” However, these arguments are tenuous when considered in light of another regulatory framework crafted precisely for the Internet age—the Digital Millennium Copyright Act (“DMCA”).

Internet media companies are already “quite good at complying with at least one government regulation.” The DMCA has, as intended, mobilized platforms to control individual users. Remarkably, “[t]he existence of the legal scheme set forth in the DMCA demonstrates that the CDA’s policy of conferring complete immunity on ISPs is not inevitable and, most significantly, not currently understood as a First Amendment requirement.” In the estimation of communications professors Nina Brown and Jonathan Peters, “[i]f there were any existing, workable model for Congress to use to regulate fake news on social media, this would be it.”

Like Section 230, the safe harbor provisions of the DMCA shield online service providers from claims—in this instance copyright infringement claims—arising from third-parties. Section 512 of the DMCA states that a service provider must adopt and reasonably implement a policy as a condition of eligibility for safe harbor protection.

---

154. Citron, supra note 12.
155. BROWN, supra note 16, at 530 (discussing the notice and takedown provisions of the Digital Millennium Copyright Act (DMCA)).
156. Tushnet, supra note 41, at 1004. Professor Citron has noted that the critique that Congress intended to encourage free speech on the Internet is divorced from the legislative history. See CDA 230: Legislative History, Electronic Frontier Foundation, https://www.eff.org/issues/cda230/legislative-history (last visited Apr. 29, 2020).
157. Brown, supra note 16, at 531 note 72 (noting that DMCA § 512 has been used as a suggested framework for legislation in the instances of regulating revenge pornography and defamation).
Consider a recent lawsuit wherein an Internet media company invoked Section 230 in light of the proposed reasonable steps approach. While the matter did not involve fake news, the analysis provides a basis for consideration. Section 230 doctrine insulated Grindr, an online dating platform, in a lawsuit alleging that the platform’s negligent design of its dating app enabled a campaign of harassment resulting from a user’s ability to impersonate another.\(^{159}\) Specifically, the amended complaint alleged that the site, whose terms of service prohibit the use of its product to impersonate, stalk, harass, or threaten, did nothing to respond to the plaintiff’s complaints.\(^{160}\) Moreover, the complaint alleged a number of design decisions that, if reasonably undertaken, would have prevented or mitigated the harm.\(^{161}\) There, a court may be unlikely to grant a motion to dismiss on Section 230 grounds under the proposed amendment, reasoning that the site lacked a reasonable process to monitor its terms of service writ large rather than because the site moderators failed to respond responsibly in the Plaintiff’s case.

With respect to moderating fake news, an Internet media company could avail itself of Section 230 safe harbors if it employed reasonable steps to monitor, identify, and remove content that did not accord with its community standards and terms of service. An argument could be made that content moderation decisions including algorithm-enabled ranking may be similar to a publisher’s editorial choices and may deserve First Amendment protection. Thus, the validity of this regulation would involve discerning whether the algorithms that the Internet media companies deploy are due First Amendment rights as a type of speech.

Amending Section 230 will likely raise concerns about censorship. Those concerns, however, may be overblown in light of online media companies’ conduct in compliance with German regulation discussed above. Moreover, the amendment’s effect of compelling platforms to adopt reasonable standards in order to retain immunity would not come to bear on any particular element of speech.

To the extent that the proposed amendment is resisted on the grounds that it contravenes the legislative intent to leave the Internet unregulated, this Article offers the proposition that “[t]he Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant-perhaps the preeminent-means through which commerce is conducted.”\(^{162}\)


\(^{160}\) Id.

\(^{161}\) Id.

\(^{162}\) Fair Hous. Council v. Roommate.com, LLC, 521 F.3d 1157, 1164 n.15 (9th Cir. 2008).
Lawrence Lessig reminds us that “[h]ow the code regulates . . . [is a] question[] that any practice of justice must focus [on] in the age of cyberspace.” Lawrence Lessig reminds us that “[h]ow the code regulates . . . [is a] question[] that any practice of justice must focus [on] in the age of cyberspace.”163 Platforms control what content appears on their services through their design choices and speech policies. Thus, it is in this currently unregulated space that Congress is afforded perhaps the most appropriate opportunity to affect behavioral change while maintaining the integrity of Section 230.165

Conclusion

Fake news presents an ever-growing problem around the globe. The First Amendment’s free speech protections and the Communications Decency Act curtail any government regulation on speech. However, that does not leave the area without regulation. The private sector needs regulatory support to bolster its efforts to find fake news and identify it for users. This can be achieved through an amendment to Section 230 that conditions immunity on compliance with technical reasonable standards to address fake news. The recommendation of the adoption of the “reasonable standards” approach advanced herein is a modest extension of current jurisprudence and would provide a balanced approach to regulating online political speech, so as to not curb free expression or censor content.

163. Id.; see also Joel R. Reidenberg, Note, Lex Informatica: The Formulation of Information Policy Rules Through Technology, 76 Tex. L. Rev. 553, 554-56 (1998) (exploring how system design choices provide sources of rulemaking and make a “useful extra-legal instrument that may be used to achieve objectives that otherwise challenge conventional laws”).
164. See Citron, supra note 12.