# ONLINE TERRORIST SPEECH, DIRECT GOVERNMENT REGULATION, AND THE COMMUNICATIONS DECENCY ACT

STEVEN BEALE†

ABSTRACT

*The Communications Decency Act (CDA) provides Internet platforms complete liability protection from user-generated content. This Article discusses the costs of this current legal framework and several potential solutions. It proposes three modifications to the CDA that would use a carrot and stick to incentivize companies to take a more active role in addressing some of the most blatant downsides of user-generated content on the Internet. Despite the modest nature of these proposed changes, they would have a significant impact.*

## INTRODUCTION

On October 31, 2017, a truck allegedly driven by Sayfullo Habibullaevic Saipov sped onto a bike path in New York City. The truck struck multiple people, killing eight of them. Saipov then allegedly emerged from the truck and brandished a paintball and pellet gun before being shot by a police officer.[1] Although investigators are still trying to determine the details of Saipov's path to radicalization, there is evidence he was radicalized by exposure to online materials created by the Islamic State in Iraq and Syria (ISIS).[2]

For years, experts have sounded warnings about how terrorists use social media and online resources to recruit, train, plan, finance, and coordinate their activities.[3] ISIS has been especially adept at using social

---

† Duke University School of Law, J.D. expected May 2019; M.A. in Political Science, The Ohio State University, December 2014; B.A. in World Politics, Hamilton College, May 2009. I would like to thank Major General Charles Dunlap as well as Professors Sara Beale, Stuart Benjamin, David Hoffman, and Christopher Schroeder for their guidance and comments.

[1] *See* Holly Yan & Dakin Andone, *Who is New York Terror Suspect Sayfullo Saipov?*, CNN (Nov. 2, 2017), http://www.cnn.com/2017/11/01/us/sayfullo-saipov-new-york-attack/index.html.

[2] *See* Nicole Chavez et al., *New York Attack Suspect Charged with Federal Terrorism Offenses*, CNN (Nov. 2, 2017), https://www.cnn.com/2017/11/01/us/new-york-attack/index.html.

[3] *See, e.g.*, Maeghin Alarid, *Recruitment and Radicalization: The Role of Social Media and New Technology*, *in* IMPUNITY, 313 (Michelle Hughes & Michael

media to spread its message of hate.[4] Indeed, on a single day in 2014, ISIS posted nearly 40,000 Tweets.[5]

The continued use of the Internet and social media by terrorists and hate groups to facilitate their activities has fueled a growing debate about whether the U.S. government should take a more aggressive role in combating online hate speech. Some have argued that the government should take a direct role in regulating online content either by classifying social media websites as public forums or reclassifying the Internet as a public utility.[6] This Article will examine these options and argue that they would actually make regulating online hate speech *more* difficult.

Consequently, the better approach to regulating online hate speech is to amend the Communications Decency Act (CDA). This Article proposes three specific changes that utilize both a carrot and sticks. The sticks would remove the current absolute liability protection for social media platforms for content posted by designated foreign terrorist organizations and individuals who claim membership in those organizations. The carrot, however, would provide a safe harbor from liability protection for companies that institute compliance programs and make reasonable efforts to remove such content.

Part I of this Article will examine the First Amendment and the CDA. It will discuss how the marketplace of ideas underpins the First Amendment. This underpinning helps to explain and justify the Supreme Court's incitement jurisprudence. This First Amendment jurisprudence, combined with the CDA's liability protection, has created an Internet where the government has almost no ability to limit hateful online content. However, companies have huge discretion to determine what content to allow on their own sites. Part II will discuss several options for the government to take a more direct, regulatory role online. It will show how

---

Miklaucic eds., 2016), http://cco.ndu.edu/Publications/Books/Impunity/Article/780274/chapter-13-recruitment-and-radicalization-the-role-of-social-media-and-new-tech/; United Nations Office on Drugs and Crime, *The Use of the Internet for Terrorist Purposes*, THE UNITED NATIONS 3–11 (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

[4] *See ISIL Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media; Hearing Before the S. Subcomm. on Investigations of the Comm. On Homeland Sec. and Gov't Affairs*, 114th Cong. (2016) (statement of Michael Steinbach, Federal Bureau of Investigation, Executive Assistant Director, National Security Branch).

[5] *How Terrorists are Using Social Media*, THE TELEGRAPH (Nov. 4, 2014, 4:02 PM), http://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html.

[6] *See infra* Part II.

direct government control of the Internet would actually impede government efforts to combat problematic online speech. Part III will discuss modifying the CDA to help diminish terrorist hate speech online. It will put forth several amendments to the CDA and then discuss and address several possible concerns to the proposal. These proposed modifications to the CDA would have a significant impact and little downside.

## I. THE FIRST AMENDMENT, THE COMMUNICATIONS DECENCY ACT, AND THE REALITY ONLINE

The U.S. provides very high protections for speech, both online and offline.[7] Free speech jurisprudence is grounded in the First Amendment, which provides that "Congress shall make no law . . . abridging the freedom of speech . . . ."[8] Despite its inclusion in the Bill of Rights, the First Amendment generated little litigation until World War I.[9]

Current First Amendment jurisprudence is grounded in the "marketplace of ideas" rationale. This rationale informs the court's jurisprudence on incitement and makes it very difficult for (1) speech to qualify as incitement and (2) the government to censor any content, including online content. The CDA provides additional protections for platform providers by absolving them of liability for user-generated content. Taken together, these three characteristics have created an environment where it is nearly impossible for the U.S. government to censor even terrorists' online speech. Conversely, private companies that control Internet platforms have a nearly unlimited ability to restrict content on their sites, although they have little incentive to do so.

### *A. The Marketplace of Ideas*

The marketplace of ideas rationale can be traced back to Justice Holmes' famous dissent in *Abrams v. United States*.[10] Justice Holmes stated that the theory behind the U.S. Constitution is "that the best test of truth is the power of the thought to get itself accepted in the competition

---

[7] *See* Alexander Tsesis, *Terrorist Speech on Social Media*, 70 VAND. L. REV. 651, 688 (2017) (noting that the U.S. "approach to free speech tends to be more libertarian than Europe's and Canada's").

[8] U.S. CONST. amend. I.

[9] *See* Alan K Chen, *Free Speech and the Confluence of National Security and Internet Exceptionalism*, 86 FORDHAM L. REV. 379, 381 (2017) (noting that "[t]he modern understanding of the free speech doctrine is only about 100 years old."); Diane Leenheer Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33 WM. & MARY L. REV. 665, 725 (1992) (stating that the Supreme Court's jurisprudence on the First Amendment was a "late bloomer").

[10] 250 U.S. 616, 624–30 (1919) (Holmes, J. dissenting).

of the market."[11] A few years later in a concurrence, Justice Brandeis posited that "[t]hose who won our independence believed that the final end of the State was to make men free to develop their faculties" and "that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth."[12]

Since then, the marketplace of ideas rationale has gained widespread acceptance on the Court.[13] Following *Abrams*, the Court has repeatedly affirmed the concept as the rationale underlying the First Amendment.[14] It noted that "[i]f there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable."[15] The marketplace of ideas rationale has been influential in the Court's Internet-related jurisprudence. For example, the Court held that portions of the CDA, as originally drafted, violated the First Amendment by chilling speech and impairing the marketplace of ideas.[16]

### *B. Incitement*

The Court's current interpretation of incitement is also relatively recent. Its early incitement jurisprudence was heavily influenced by the current events of the day, namely World War I.[17] In these early cases, the

---

[11] *Id.* at 630.

[12] Whitney v. California, 274 U.S. 357, 375 (1927).

[13] *See* Joseph Blocher, *Institutions in the Marketplace of Ideas*, 57 DUKE L.J. 821, 825 (2008) (noting that "First Amendment doctrine has carried Holmes's laissez-faire marketplace banner more or less faithfully since Abrams . . .").

[14] *See, e.g.*, Cohen v. California, 403 U.S. 15, 24 (noting that "The constitutional right of free expression is . . . . designed and intended to remove governmental restraints from the arena of public discussion, putting the decision as to what views shall be voiced largely into the hands of each of us, in the hope that use of such freedom will ultimately produce a more capable citizenry and more perfect polity . . ." (citing Whitney v. California, 274 U.S. 357, 375–77 (1927)); N.Y. Times Co. v. Sullivan, 376 U.S. 254, 269 (1964) (quoting Roth v. United States, 354 U.S. 476, 484) (stating that the constitutional safeguard of freedom of expression "was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people.").

[15] Texas v. Johnson, 491 U.S. 397, 414 (1989) (holding that flag burning was protected under the First Amendment).

[16] Reno v. ACLU, 521 U.S. 844, 885 (1997).

[17] *See, e.g.*, Schenck v. United States, 249 U.S. 47, 52 (1919) (citing Aikens v. Wisconsin, 195 U.S. 194 (1904)) (noting that while "in ordinary times" the defendant's advocacy against the draft would be constitutionally protected, "the character of every act depends upon the circumstances in which it is done."); Frohwerk v. United States, 249 U.S. 204, 209 (1919) (stating that "the circulation of the paper [which criticized the war effort] was in quarters where a little breath would be enough to kindle a flame . . . .").

Court did not require the government show actual or even imminent harm. Rather, a successful conviction could be based on showing that the defendant's actions "had as their natural tendency and reasonably probable effect" lawless action.[18]

However, in its landmark decision *Brandenburg v. Ohio*, the Court shifted course, adopting a three-part test to determine if speech qualified as unprotected incitement, requiring the speech be (1) directed toward inciting or producing (2) imminent lawless actions and (3) likely to incite or produce such actions.[19] Since *Brandenburg*, the Court has clarified that imminent lawless actions must be more than "advocacy of illegal action at some indefinite future time"[20] and sooner than "weeks or months" after the speech.[21]

The *Brandenburg* test is very difficult for the government to pass. For example, in one case a boycott organizer threatened to have those who violated the boycott "disciplined," saying that "[i]f we catch any of you going in any of them racist stores, we're gonna break your damn neck."[22] Though boycott violators were publicly identified, called traitors,[23] and allegedly subjected to violence or threats,[24] the Court held that the defendant's actions were constitutionally protected under the First Amendment.[25] Moreover, "[t]he mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it . . . ."[26] Therefore, the *Brandenburg* conditions are very difficult to meet.

---

[18] Debs v. United States, 249 U.S. 211, 216 (1919). *See also* Gitlow v. New York, 268 U.S. 652, 669 (1925) (reasoning that even though the defendants' alleged criminal anarchy conviction for publishing a manifesto urging a communist revolution by mass industrial revolts did not cause "immediate danger," the conviction was proper because "[a] single revolutionary spark may kindle a fire that, smouldering for a time, may burst into a sweeping and destructive conflagration.").

[19] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curium).

[20] Hess v. Indiana, 414 U.S. 105, 108 (1973) (holding that defendant's statement during an anti-war protest of "We'll take the fucking street later (or again)" while standing close to law enforcement officials was not incitement to imminent illegal action).

[21] NAACP v. Claiborne Hardware Co., 458 U.S. 886, 928 (1982).

[22] *Id.* at 902.

[23] *Id.* at 903–04.

[24] *Id.* at 904–06.

[25] *Id.* at 928 (stating that "[s]trong and effective extemporaneous rhetoric cannot be nicely channeled in purely dulcet phrases. An advocate must be free to stimulate his audience with spontaneous and emotional appeals . . . . When such appeals do not incite lawless action, they must be regarded as protected speech.").

[26] Ashcroft v. Free Speech Coal., 535 U.S. 234, 253 (2002).

### *C. The Communications Decency Act*

The CDA serves as another significant bar to limiting online speech. It 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."[27] It defines "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[28] Website operators, such as YouTube, Facebook, and Twitter, can simultaneously be both operators and content providers.[29]

The CDA also specifically notes under its findings that it was inspired by the marketplace of ideas rationale.[30] The CDA provides a significant additional protection to online speech that supplements the already very strong protections provided by the First Amendment and the Supreme Court's current jurisprudence.

### *D. Online Hate Speech*

Online speech is defined by two main attributes. First, the government has little independent ability to regulate or censor even the most egregious online content. Second, companies hosting such content have a nearly unlimited ability to censor, or not censor, whatever content they want to on their platforms. Not surprisingly, these conditions have led to a world in which victims of hate speech or terrorism that is facilitated by online content have little recourse.

Despite the CDA's protections, lawsuits have sought to hold social media websites responsible for some content posted by users. In particular, several cases have attempted to hold social media companies liable for deaths in terrorist attacks under the Anti-Terrorism Act. In these cases, the plaintiffs have alleged that social media companies provided material support to terrorists who then carried out attacks, including an attack on government contractors in Jordan[31] and terrorist attacks in Europe.[32] For example, one pending complaint alleges that even though Twitter knew that ISIS was a designated Foreign Terrorist Organization,

---

[27] 47 U.S.C. § 230(c).
[28] 47 U.S.C. § 230(f)(3).
[29] *See* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008).
[30] 47 U.S.C. § 230(a)(3) (stating that "[t]he Internet and other interactive computer services offer a forum for a true diversity of political discourse . . .").
[31] Fields v. Twitter, 217 F. Supp. 3d 1116, 1118 (N.D. Cal. 2016), *aff'd* No. 16-17165 2018 WL 626800 (9th Cir 2018).
[32] Cain v. Twitter, 2017 U.S. Dist. LEXIS 62724, at *5 (S.D.N.Y. Apr. 25, 2017).

"Twitter has for years knowingly provided its Services to ISIS, its members, organizations owned or controlled by ISIS, and organizations and individuals that provide financing and material support to ISIS."[33] Moreover, the complaint alleges that Twitter helped ISIS conduct past terrorist attacks by aiding ISIS' internal and external communications, planning, recruiting, organizing, training, and funding.[34] While the court has not yet ruled on the merits of the that case, another federal district court dismissed a comparable set of claims, holding that the CDA shielded Twitter from liability since it was not an information content provider.[35]

Additionally, in *Klayman v. Zuckerburg* the D.C. Circuit dismissed a similar claim against Facebook.[36] In this case, the plaintiff alleged intentional assault and negligent breach of duty of care for Facebook's failure to promptly remove a page entitled the "Third Palestinian Intifada."[37] With more than 360,000 members, the page called for an uprising against the Israeli occupation of Palestinian areas, and proclaimed that "Judgment Day" would only arrive when "Muslims have killed all the Jews."[38] Klayman alleged both he and the Israeli government had warned Facebook about the page, but Facebook had failed to promptly remove it. In affirming the district court's dismissal, the D.C. Circuit held that the CDA barred Facebook's liability since Facebook was not the information content provider.[39]

Despite such pressure, efforts to make significant amendments to the CDA have not yet been successful. Congress recently passed a narrow amendment to the CDA that removes the CDA's liability protections for sex-trafficking.[40] However, the bill is very narrowly tailored and does not apply to online hate or terrorist speech.[41]

Consequently, the U.S. government has engaged in almost no regulation of online hate speech or incitement on non-government websites. Conversely, most Internet companies have broad power to police

---

[33] Complaint at 382–83, Cain v. Twitter, 2017 U.S. Dist. LEXIS 62724 (S.D.N.Y. Apr. 25, 2017).
[34] *Id.* at 209–12.
[35] *Fields*, 217 F. Supp. 3d at 1118. The court in *Cain v. Twitter* has not yet decided the case on the merits; it has merely allowed the case to be transferred from Southern District of New York to the Northern District of California. Cain v. Twitter, 2017 U.S. Dist. LEXIS 62724, at *18 (S.D.N.Y. Apr. 25, 2017).
[36] Klayman v. Zuckerberg, 753 F.3d 1354, 1359–60 (2014).
[37] *Id*. at 1356.
[38] *Id.*
[39] *Id.* at 1357–60.
[40] *See* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, P.L. 115-164, § 4(a), 132 Stat. 1253, 1254 (2018).
[41] *See id.*

what information, including user-generated information, is on their websites. Most websites and web services have user agreements that allow platforms to determine the type of content they allow on their websites.[42] Thus, private companies have full discretion regarding whether to censor virtually any content their users post.

Companies' ability to choose whether or not to censor has been especially apparent in the wake of a white nationalist rally in Charlottesville. Even before the Charlottesville rally and its accompanying violence, Airbnb kicked users off its platform that it thought were attending the rally.[43] Following the violence in Charlottesville, the web-performance and security company Cloudflare stopped providing services to the Daily Stormer, a prominent neo-Nazi and white supremacist news and commentary website, effectively taking it offline. In a statement to his staff, the CEO wrote "[l]iterally, I woke up in a bad mood and decided someone shouldn't be allowed on the Internet."[44] Additionally, Twitter and Facebook removed accounts related to white supremacists,[45] PayPal

---

[42] *See, e.g.*, *Terms of Service*, TWITTER (Oct. 2, 2017), https://twitter.com/en/tos#usUsing (noting that "[w]e reserve the right to remove Content alleged to be infringing without prior notice, at our sole discretion, and without liability to you"); *Terms of Service*, FACEBOOK (Jan. 30, 2015), https://www.facebook.com/terms.php ("[w]e can remove any content or information you post on Facebook if we believe that it violates this Statement or our policies.").

[43] Kyle Swenson, *Airbnb Boots White Nationalists Headed to 'Unite the Right' Rally in Charlottesville*, THE WASH. POST (Aug. 8, 2017), https://www.washingtonpost.com/news/morning-mix/wp/2017/08/08/airbnb-boots-white-nationalists-headed-to-unite-the-right-rally-in-charlottesville/?utm_term=.0923547c9fc4.

[44] Kate Conger, *Cloudflare CEO on Terminating Service to Neo-Nazi Site: 'The Daily Stormer are Assholes,'* GIZMODO (Aug. 16, 2017, 6:00 PM), https://gizmodo.com/cloudflare-ceo-on-terminating-service-to-neo-nazi-site-1797915295; *see also* Matthew Prince, *Why We Terminated Daily Stormer*, CLOUDFLARE (Aug. 16, 2017) https://blog.cloudflare.com/why-we-terminated-daily-stormer/ (discussing why Cloudflare removed the Daily Stormer).

[45] *See* Rob Price, *Charlottesville is a Tipping Point in Silicon Valley's Approach to Speech*, BUSINESS INSIDER (Aug. 17, 2017, 9:16 AM), http://www.businessinsider.com/tech-companies-crack-down-hate-speech-charlottesville-2017-8; *see also* Mark Zuckerberg, FACEBOOK (Aug. 16, 2017), https://www.facebook.com/zuck/posts/10103969849282011 (Facebook founder Mark Zuckerberg posted on his Facebook page a message condemning the violence and stating that "we've always taken down any post that promotes or celebrates hate crimes or acts of terrorism -- including what happened in Charlottesville.").

blocked white supremacists from using its services,[46] and a dating app even banned the account of a prominent white supremacist.[47]

So, while the CDA prevents individuals from holding private companies liable for third party content on their sites, the companies themselves have almost unlimited discretion about whether to censor user-generated content on their sites. This is concerning for several reasons. First, although private companies have the ability to take down problematic content, they often act after-the-fact and in a very limited manner. This is no surprise: searching for content costs money and removes users from the platform, both of which harm profits. Consequently, platform providers have little incentive to tightly police user-generated content on their sites. Moreover, there are often some platforms that either sympathize with problematic speech or ignore the negative consequences of the speech in a quest to serve a niche market.[48] Additionally, allowing platforms, especially the largest platforms that are increasingly central to many people's lives, to have sole discretion over what content is allowed and what is prohibited is anti-democratic.[49] The more important and central to modern life such sites become, the more worrying it becomes for large platforms to lack democratic accountability.

## II. THE PUBLIC FORUM DOCTRINE AND THE DOWNSIDES OF DIRECT GOVERNMENT REGULATION

This situation has led to calls for greater direct government involvement and regulation of the Internet. While there are several ways the government could more directly regulate online content, the Public Forum Doctrine actually makes such direct government control and regulation a poor way to reduce online hate speech.

### *A. Direct Government Regulation?*

There are several possibilities for direct government regulation of online platforms. One possibility is for the government to classify some

---

[46] Matt Stevens, *After Charlottesville, Even Dating Apps are Cracking Down on Hate*, N.Y. TIMES, Aug. 25, 2017, at B3.
[47] *Id.*
[48] For example, the Stop Enabling Sex Traffickers Act of 2017 was largely motivated by the actions of Backpage.com, a website that allegedly "create[s] a marketplace for the sale and purchase of trafficking victims . . . ." *See* SENATOR ROBERT PORTMAN, STOP ENABLING SEX TRAFFICKERS ACT OF 2017 1 (2017), *available at* https://www.portman.senate.gov/public/index.cfm/files/serve?File_id=B3F5988E-C4BD-4ACE-A881-6EB9068325B9.
[49] John Herrman, *How Hate Groups Forced Online Platforms to Reveal Their True Nature*, N.Y. TIMES, Aug. 27, 2017, at MM18 (noting that "[d]espite their participatory rhetoric, social platforms are closer to authoritarian spaces than democratic ones.").

websites as public forum. In his opinion in *Packingham v. North Carolina*, Justice Kennedy suggested that the Internet, and social media in particular, may be becoming "essential venues for public gatherings . . . ."[50] Kennedy went so far as to call social media "the modern public square" because it allows individuals to amplify their speech, including political speech.[51] Justice Kennedy did not discuss the potential impact of classifying some websites as public forums on online hate speech or incitement.

A second possibility is to classify certain websites or web services that are increasingly essential to many people's lives, such as Facebook and Google, as public utilities. This idea has been floated by those on both ends of the political spectrum[52] as well as discussed by some in the technology community.[53] The idea is simply that the Internet is essential to modern life, much like electricity. If classified as a public utility, the government could theoretically more easily regulate the largest Internet companies.

### *B. Public Forum Doctrine and Direct Government Regulation*

The Supreme Court uses a forum-based approach to analyze the level of scrutiny and restrictions the government may place on speech in government-controlled areas.[54] Traditional and designated public forums are locations either historically used as or designated by the government as places for public assembly, communications, or other expressive activity.[55] They include, but are not limited to, parks and sidewalks.[56]

Limited public forums are created for a specific purpose by the government.[57] In a limited public forum, the government "must respect the lawful boundaries it has itself set" and cannot prohibit activities related to the purpose of the forum.[58] Some locations are also designated as

---

[50] Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017).
[51] *Id.* at 1737 (noting that social media websites "allow a person with an Internet connection to 'become a town crier with a voice that resonates farther than it could from any soapbox'" (quoting Reno v. ACLU, 521 U.S. 844, 870 (1997)).
[52] *See* Robinson Meyer, *What Steve Bannon Wants to Do to Google*, THE ATLANTIC (Aug. 1, 2017), https://www.theatlantic.com/technology/archive/2017/08/steve-bannon-google-facebook/535473/.
[53] *See* Danah Boyd, *Facebook is a Utility, Utilities Get Regulated*, APOPHENIA (May 15, 2010), http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html.
[54] Int'l Soc'y for Krishna Consciousness v. Lee, 505 U.S. 672, 678 (1992).
[55] Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983) (quoting Hague v. CIO, 307 U.S. 496, 515 (1939)).
[56] *Id*.
[57] *See* Rosenberger v. Rector & Visitors of the Univ. of Va., 515 U.S. 819, 829 (1995) (noting that a limited public forum is created for a specific purpose).
[58] *Id*.

nonpublic forums. In such locations, the government may limit speech and activities to those "compatible with the intended purpose of the property."[59] Finally, other areas, such as government funding programs, are classified as not forums at all. When there is no forum, the government may advocate for whatever policy it pleases.[60]

If subject to direct government control, the Internet would clearly be a forum; for the Internet to be a non-public forum, most non-governmental content would have to be removed from the Internet, a scenario almost impossible to imagine.[61] Additionally, a limited public forum designation would probably too narrowly encapsulate the range of legal activity that is allowed online: limited public forums are generally created by the government for specific purposes and allow only selective access.[62]

Consequently, the Internet would likely be classified as a public forum. Classifying certain websites like social media platforms as public forum, as Justice Kennedy suggests in *Packingham*, would make government regulation of hate speech much more difficult. As Justice Alito pointed out in his concurrence in *Packingham*, classifying social media as public forum is "bound to be interpreted by some" as preventing governmental regulation of social media that would otherwise be permissible.[63] The government is very limited in the ways it can restrict speech in public forums since there is an especially strong interest in protecting speech in those spaces.[64] Government regulation of speech in a public forum is subject to strict scrutiny,[65] which means that the regulation must serve a compelling government interest and be narrowly drawn.[66] The strict scrutiny analysis under the First Amendment has traditionally

---

[59] *Perry*, 460 U.S. at 49.
[60] *See* Rust v. Sullivan, 500 U.S. 173, 193 (1991) ("The Government can . . . selectively fund a program to encourage certain activities it believes to be in the public interest, without at the same time funding an alternative program which seeks to deal with the problem in another way. In so doing, the Government has not discriminated on the basis of viewpoint; it has merely chosen to fund one activity to the exclusion of the other.").
[61] *See* Ark. Educ. Television Comm'n v. Forbes, 523 U.S. 666, 678 (1998); *Perry*, 460 U.S. at 47 (noting that non-public forums generally consist of largely government activity or activity very closely related to government action).
[62] *See* Cornelius v. NAACP Legal Def. & Educ. Fund, 473 U.S. 788, 804–06 (1985).
[63] Packingham v. North Carolina, 137 S. Ct. 1730, 1738 (2017) (Alito, J. concurring).
[64] McCullen v. Coakley, 134 S. Ct. 2518, 2529 (2014).
[65] *See Perry*, 460 U.S. at 45.
[66] *Cornelius*, 473 U.S. at 800.

been very difficult to pass.[67] Therefore, if the Internet were classified as a public forum, any government restrictions would face a very high bar.

## III. MODIFYING THE COMMUNICATIONS DECENCY ACT

### *A. Proposal*

Since courts have interpreted the CDA as giving online platforms, including social media companies, blanket liability protection, there is currently little incentive for companies to remove content. In response to specific and high-profile instances, like the violence in Charlottesville, platforms may clamp down on some particularly egregious speech or users. Otherwise, platforms lack strong incentivizes to act—any actions they take would reduce subscribers and hurt their bottom line. This has created an Internet where hate speech is too often left unchecked. To best address this problem, this Article suggests three amendments to the CDA. Taken together, these changes would lessen terrorist speech online while having a negligible impact on other speech. Compliance with these proposals would also not unduly burden Internet platforms.

First, platforms that fail to promptly take down the official accounts of designated Foreign Terrorist Organizations (FTOs) operating on their websites should lose all liability protections under the CDA. Platforms could have a duty to remove such content under two circumstances. First, law enforcement could notify the platform of the FTO account.[68] While notification is an excellent first step, waiting for notification does not incentivize platforms to actively seek out FTO accounts. Moreover, companies are often in the best position to mine their own data, and they have demonstrated a sophisticated ability to identify traits about customers.[69] Consequently, platforms should also have a duty to make reasonable efforts to monitor their platforms for FTO accounts.

There is no reasonable justification for allowing FTOs to amplify their messages of hate on online platforms. If a platform knows the FTO is using its service and fails to stop the FTO, the platform may already be

---

[67] *See* David Cole, *The First Amendment's Borders: The Place of Holder v. Humanitarian Law Project in First Amendment Doctrine*, 6 HARV. L. & POL'Y REV. 147, 148 (2012).

[68] *See* Michelle Roter, Note, *With Great Power Comes Great Responsibility: Imposing a "Duty to Take Down" Terrorist Incitement on Social Media*, 45 HOFSTRA L. REV. 1379, 1404–08 (2017) (proposing that social media companies have a duty to take down terrorist accounts only after law enforcement notification).

[69] *See, e.g.*, Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 19, 2012, at MM30 (discussing Target's use of data mining to determine a customer was pregnant before her family knew about the pregnancy).

violating the terrorist material support statute.[70] It makes little sense, then, for platforms to have civil liability protection when they potentially have criminal liability. Removing the CDA's civil liability shield is likely to provide a greater incentive for companies to modify their behavior than criminal penalties because private parties are often more likely to sue than the government.

Additionally, designation as an FTO reflects the political branches' determination that the group is a foreign terrorist organization and harmful to U.S. interests. Although law enforcement and intelligence agencies may gain some intelligence from terrorist accounts and websites,[71] there is little reason to think that this change to the CDA would significantly impair intelligence gathering. Many other means of gathering intelligence would remain, including examining the statements such organizations make to the news media, signals intelligence, or other traditional intelligence means. What such a prohibition would do is make it harder for FTOs to spread their messages, solicit donations, and recruit new adherents.

Consequently, to make it much more difficult for FTOs to spread their messages, Congress should amend the CDA to add the following language, or language to a similar effect:

> § 230(c)(3): An interactive computer service provider may be treated as the publisher or speaker of such content if the provider knows or should have known the content was provided by a designated foreign terrorist organization under 8 U.S.C. § 1189.

Second, the CDA should no longer provide liability protection for companies that fail to remove user-generated content of individuals who explicitly self-identify as members of an FTO. Similar to identifying FTO accounts, platforms should likely have little trouble finding such content since this exception to the CDA's blanket protection would only apply to individuals who explicitly self-identified as members of FTOs. Moreover, this provision would be narrowly tailored to only apply to individuals that meet the demanding standards of "personnel" under 18 U.S.C. 2339B(h).[72]

---

[70] *See id.*

[71] *See* Benjamin Wittes & Zoe Bedell, *Tweeting Terrorists, Part III: How Would Twitter Defend Itself Against a Material Support Prosecution*, LAWFARE (Feb. 14, 2016, 7:16 PM), https://www.lawfareblog.com/tweeting-terrorists-part-iii-how-would-twitter-defend-itself-against-material-support-prosecution (noting that there may be security benefits in "being able to follow what terrorist groups are thinking and trying to communicate to their followers[.]") .

[72] The statute provides that:

> No person may be prosecuted under this section in connection with the term 'personnel' unless that person has knowingly provided, attempted

Removing blanket liability protection for user-generated content authored by explicitly self-identified members of FTOs would incentivize companies to proactively remove the most problematic user-generated content on their platforms. Consequently, the CDA should be modified so that it includes the following language:

> § 230(c)(4): U.S.C. § 230(c) shall not be interpreted as providing interactive computer service providers immunity from private civil suits for information content authored by publishers or speakers who
>
> > (A) publicly identify themselves as members of an organization that has been designated as a foreign terrorist organization under 8 U.S.C. § 1189,
> >
> > (B) qualify as "personnel" under 18 U.S.C. 2339B(h), and
> >
> > (C) the information service provider failed to promptly remove such content.

Finally, as long as platforms make reasonable, good faith efforts, they should continue to enjoy liability protection for user-generated content.[73] One way to determine if platforms are taking reasonable steps would be to create a certification program. Such a program could be self-certified and similar to the U.S.-E.U. Privacy Shield[74] or the Department of Commerce's National Institute of Standards and Technology Critical Infrastructure for Cybersecurity Framework.[75] Since technology changes so quickly, the requirement should be broad. To create such a safe harbor, the CDA could include the following language:

---

> to provide, or conspired to provide a foreign terrorist organization with 1 or more individuals (who may be or include himself) to work under that terrorist organization's direction or control or to organize, manage, supervise, or otherwise direct the operation of that organization. Individuals who act entirely independently of the foreign terrorist organization to advance its goals or objectives shall not be considered to be working under the foreign terrorist organization's direction and control.

18 U.S.C. § 2339B(h) (2015).

[73] *See* Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 419 (2017) (proposing a modification to the CDA that requires companies to make reasonable efforts to remove unlawful user-generated content on their platforms to receive liability protection).

[74] *See Welcome to the Privacy Shield*, PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/welcome (last visited Dec. 9, 2017).

[75] *See Cybersecurity Framework*, NAT'L INST. OF STANDARDS AND TECH., https://www.nist.gov/cybersecurity-framework (last visited Dec. 10, 2017).

> § 230(c)(5): Any provider of an interactive computer service that has made good faith efforts to comply with 47 U.S.C. §230(c)(3) and (4) shall not be deemed to be a publisher or speaker. Such reasonable efforts may include a self-certification scheme that satisfies requirements approved by the Department of Commerce.

### *B. Discussion*

Together, these three amendments would have a significant impact without raising many of the complications of some other suggested modifications to the CDA. First, the lack of direct government regulation would avoid the stringent forum analysis required by reclassifying the Internet as a public forum or utility.

In contrast to some other proposals,[76] these measures would also be unlikely to raise other First Amendment challenges. Even assuming these proposals would be classified as restrictions on speech and not conduct,[77] they would still almost certainly be constitutional under *Humanitarian Law Project* (*HLP*). In *HLP*, the Court held that it was permissible for the government to bar organizations from engaging in activities such as training FTOs in "how to use humanitarian and international law to peacefully resolve disputes."[78] The Court emphasized the strong government "interest in combating terrorism" could outweigh burdens on speech.[79] These proposals here clearly address a very strong interest in the government preventing terrorists from using platforms to organize, recruit, train, and fundraise. Moreover, they would merely remove protections for platforms that knew or should have known about activity much more directly related to foreign terrorism than the activities the Court found the government could restrict in *HLP*. In *HLP*, the Court also showed great deference to the political branches' determination of

---

[76] *See* Eric Posner, *ISIS Gives Us No Choice But to Consider Limits on Speech*, SLATE (Dec. 15, 2015, 5:37 PM), http://www.slate.com/articles/news_and_politics/view_from_chicago/2015/12/isis_s_online_radicalization_efforts_present_an_unprecedented_danger.html (proposing a law that that the author acknowledges would likely be unconstitutional under current doctrine that would make it a crime to access or share links of "websites that glorify, express support for, or provide encouragement for ISIS or support recruitment by ISIS"); Citron & Wittes, *supra* note 73, at 411 (noting that "[u]nless the [Supreme] Court upends the table, it is hard to imagine a retreat from the broad-sweeping interpretation of § 230 adopted in the state and lower federal courts.").

[77] *See* Holder v. Humanitarian Law Project, 561 U.S. 1, 26–28 (2010) (discussing when to apply the more stringent First Amendment speech analysis and when to apply the less stringent conduct analysis).

[78] *Id.* at 36 (quoting Humanitarian Law Project v. Mukasey, 552 F.3d 916, n. 1 (9th Cir. 2009)).

[79] *Id.* at 28–30.

what measures were needed to protect national security.[80] If Congress amended the CDA, and the president approved the changes, the Court might show this deference again. Like the statute in question in *HLP*, the proposed provision is also very limited and applies to only designated foreign terrorist organizations.[81] Additionally, the measures here would not impose criminal liability, and would merely remove a shield precluding civil liability.

Moreover, this proposal is very narrowly tailored. Speech that promoted similar end goals (i.e. the political goals of FTOs), but simply was authored by those not affiliated with the FTO, would retain complete liability protection under the CDA. Consequently, these proposals would merely incentivize platforms to take proactive measures to remove some of the worst content on their websites but would not chill other speech. Additionally, in recognition of the sheer volume of user-generated content posted on their sites, this proposal offers companies complete liability protection if they make reasonable efforts. Platforms would also only lose complete liability protection for content authored by self-proclaimed members of FTOs; any private plaintiffs intending to sue the platforms would still have to prove the platform had a duty to remove the content and the platform's failure to remove the content caused injury.

Removing the nearly unlimited protections the CDA provides Internet platforms would not lead to the destruction of the Internet as we know it. It has been noted that "[i]n the technology world, § 230 of the CDA is a kind of sacred cow–an untouchable protection of near-constitutional status."[82] However, there is a growing realization that the current regime is not adequately policing the most problematic online content, and Congress has recently acted to make minor changes to the CDA.[83] This initial Congressional action could facilitate further changes to the CDA.[84] Additionally, the changes proposed here are modest and clearly defined. Companies would receive safe harbor protections when they make reasonable efforts to comply. Moreover, the amount required to be done to receive the safe harbor protection could vary by the size of the platform; so, small platforms could have significantly lower burdens.

---

[80] *Id.* at 33–34 (noting that "[t]hat evaluation of the facts by the Executive, like Congress's assessment, is entitled to deference. This litigation implicates sensitive and weighty interests of national security and foreign affairs.").
[81] *See id.* at 35.
[82] Citron & Wittes, *supra* note 73, at 409.
[83] *See* Alina Selyukh, *Section 230: A Key Legal Shield For Facebook, Google Is About To Change*, NAT'L PUB. RADIO (Mar. 21, 2018, 5:11 AM), https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change.
[84] *See id.*

Consequently, there's no reason to think the sky would fall if the CDA is modified a small amount as this Article proposes.

These proposals also avoid the imposition of new criminal penalties on companies that fail to adhere to the current minimal legal requirements to take down third party content.[85] Additional criminal penalties are likely to result in a significant backlash from technology companies, harming the feasibility of the plan. These proposals simply allow more moderate civil penalties in addition to the existing criminal penalties under the Terrorist Material Support statutes. Consequently, they would provide an intermediate civil enforcement mechanism when criminal penalties are inappropriate or not purused.

Identifying the official FTO accounts and the accounts of those who specifically self-identify as FTO members would be relatively straightforward. FTOs are a distinct, easily enforceable category since they are identified by the State Department.[86] While there are some fake or copycat accounts, many FTO accounts are readily identifiable.[87] Platforms are also adept as mining their own data[88] and there are already companies that specialize in filtering user-generated content[89] that could likely develop methods to filter for FTO accounts. Moreover, companies would receive safe harbor protections when they made reasonable efforts to comply, protecting them from liability stemming from difficult to identify accounts.

While they do not restrict as much content as some would like, these proposals are probably close to the outer limits of what would be allowed under current First Amendment jurisprudence. Despite the modest

---

[85] *See* Susan Klein & Crystal Flinn, *Social Media Compliance Programs and the War Against Terrorism*, 8 HARV. NAT'L SEC. J. 53, 56–57 (2017) (proposing a law requiring social media companies "institute compliance programs that discover and report terrorist activity at the earliest possible opportunity," and companies that failed to comply would be subject to criminal penalties but receive leniency at sentencing); Ronbert H. Schwartz, Comment, *Laying the Foundation for Social Media Prosecutions Under 18 U.S.C. § 2339B*, 48. LOY. U. CHI. L.J. 1181, 1212 (2017) (proposing an amendment to 18 U.S.C. § 2339A, which deals with terrorist material support, to "include the provision of a social media platform." The statute includes both civil and criminal penalties).

[86] *See* Foreign Terrorist Organizations, UNITED STATES DEPARTMENT OF STATE, https://www.state.gov/j/ct/rls/other/des/123085.htm (last visited Dec. 9, 2017).

[87] *See* Zoe Bedell and Benjamin Wittes, *Tweeting Terrorists, Part I: Don't Look Now But a Lot of Terrorist Groups are Using the Twitter*, LAWFARE (Feb. 14, 2016, 5:05 PM), https://www.lawfareblog.com/tweeting-terrorists-part-i-dont-look-now-lot-terrorist-groups-are-using-twitter.

[88] *See* Duhigg, *supra* note 69.

[89] See SIGHT ENGINE, https://sightengine.com/ (last visited Mar. 25, 2018).

nature of the proposed changes, they would have a real impact. Companies have been at pains to point out how much they rely on the CDA's liability protections.[90] Unlike some proposals that encourage companies to bury their heads in the sand,[91] by threatening to remove the complete liability protections they enjoy under the CDA these proposed amendments would incentivize platforms to take an active role in combating some of the most problematic online speech. Importantly, these changes would likely encourage more platforms to institute internal mechanisms to search for truly problematic content. Consequently, platforms may err on the side of caution and restrict more problematic content than these proposals would in actuality require. By keeping the government's role in policing online content minimal, these proposals would also avoid significant concerns about government censorship.

## IV. CONCLUSION

For all of its positives, there is a dark side to the Internet. Not enough is being done to limit truly harmful online speech. But, it is no surprise that little is being done. The First Amendment and the Supreme Court's jurisprudence make it very difficult to prosecute incitement. Moreover, the CDA offers Internet platforms complete liability protection for user-generated content. Platforms have a natural tendency to focus on profits instead of potentially banning some of their users. These three factors all push in the same direction and have created an Internet with too much harmful speech.

The most effective way to address this problem is to incentivize platforms to be part of the solution. The proposals here utilize both a carrot and a stick: they offer continued blanket liability protection only on the condition that platforms seriously commit to policing the worst of the worst user-generated content on their sites. The additional actions companies would have to take under these proposals would be modest but would go a long way towards addressing some of the very serious downsides of the current regime.

---

[90] *See* Susan Molinari, *Google's Fight Against Human Trafficking*, GOOGLE: THE KEYWORD (Sept. 7, 2017), https://www.blog.google/topics/public-policy/googles-fight-against-human-trafficking/; Nitasha Tiku, *The Sex Trafficking Fight Could Take Down a Bedrock Tech Law*, WIRED (Sept. 20, 2017, 7:00 AM), https://www.wired.com/story/tech-firms-open-to-changing-law-to-combat-sex-trafficking/.

[91] *See* S. 2372, 114th Cong. (2015) (proposing a bill that requires companies with "actual knowledge of any terrorist activity" notify the government "as soon as reasonably possible," but providing no incentive for companies to actually look for the content).