

6-28-2019

## "Maybe Someone Dies": The Dilemma of Domestic Terrorism and Internet Edge Provider Liability

Emily B. Tate

*Boston College Law School*, [emily.tate@bc.edu](mailto:emily.tate@bc.edu)

Follow this and additional works at: <https://lawdigitalcommons.bc.edu/bclr>

 Part of the [Communications Law Commons](#), [Internet Law Commons](#), and the [National Security Law Commons](#)

---

### Recommended Citation

Emily B. Tate, *"Maybe Someone Dies": The Dilemma of Domestic Terrorism and Internet Edge Provider Liability*, 60 B.C.L. Rev. 1731 (2019), <https://lawdigitalcommons.bc.edu/bclr/vol60/iss6/7>

This Notes is brought to you for free and open access by the Law Journals at Digital Commons @ Boston College Law School. It has been accepted for inclusion in Boston College Law Review by an authorized editor of Digital Commons @ Boston College Law School. For more information, please contact [nick.szydowski@bc.edu](mailto:nick.szydowski@bc.edu).

# “MAYBE SOMEONE DIES”: THE DILEMMA OF DOMESTIC TERRORISM AND INTERNET EDGE PROVIDER LIABILITY

**Abstract:** In the aftermath of a string of highly publicized violent attacks motivated by far-right extremism, the public spotlight has swung its harsh light over tech companies—particularly social media platforms—for hosting extremism and allegedly facilitating radicalization online. With commentators across the political spectrum searching for solutions to a growing problem, the rumbling discourse has inevitably pivoted toward those platforms, with some suggesting that they should be liable for the content they host. Federal terrorism law and § 230 of the Communications Decency Act pose seemingly insurmountable hurdles to this end, but both recent congressional challenges to the CDA and increasingly creative legal arguments against it may eliminate it as a barrier. This Note argues that although radicalization on the Internet poses grave safety concerns, the law may find compromise without eroding the CDA. This Note first analyzes the massive ramifications of imposing liability on the Internet writ large, then proposes intermediate solutions via amending federal terrorism law that will do the least harm to the Internet ecosystem while attempting to solve a growing problem of violence.

## INTRODUCTION

On a warm afternoon in August of 2017, James Fields rammed his car through a crowd of people.<sup>1</sup> The crowd had just finished protesting against the white supremacist “Unite the Right” rally in Charlottesville, Virginia, but as they marched peacefully away on the street, Fields turned onto the block, reversed, then plowed his Dodge Challenger through the crowd.<sup>2</sup> The attack was brutal, hurtling people over the car, leaving thirty-five injured on the pavement, and killing a young woman named Heather Heyer.<sup>3</sup> Fields

---

<sup>1</sup> Paul Duggan, *Charge Upgraded to First-Degree Murder for Driver Accused of Ramming Charlottesville Crowd*, WASH. POST (Dec. 14, 2017), [https://www.washingtonpost.com/local/crime/driver-accused-of-plowing-into-charlottesville-crowd-killing-heather-heyer-due-in-court/2017/12/13/6cbb4ce8-e029-11e7-89e8-edec16379010\\_story.html](https://www.washingtonpost.com/local/crime/driver-accused-of-plowing-into-charlottesville-crowd-killing-heather-heyer-due-in-court/2017/12/13/6cbb4ce8-e029-11e7-89e8-edec16379010_story.html) [<https://perma.cc/8HUV-YTMF>] [hereinafter Duggan, *Charge Upgraded*].

<sup>2</sup> *Id.*

<sup>3</sup> Paul Duggan, *Neo-Nazi Sympathizer Pleads Guilty to Federal Hate Crimes for Plowing Car into Protesters at Charlottesville Rally*, WASH. POST (Apr. 1, 2019), [https://www.washingtonpost.com/local/public-safety/neo-nazi-sympathizer-pleads-guilty-to-federal-hate-crimes-for-plowing-car-into-crowd-of-protesters-at-unite-the-right-rally-in-charlottesville/2019/03/27/2b947c32-50ab-11e9-8d28-f5149e5a2fda\\_story.html](https://www.washingtonpost.com/local/public-safety/neo-nazi-sympathizer-pleads-guilty-to-federal-hate-crimes-for-plowing-car-into-crowd-of-protesters-at-unite-the-right-rally-in-charlottesville/2019/03/27/2b947c32-50ab-11e9-8d28-f5149e5a2fda_story.html) [<https://perma.cc/BVH9-W2EK>].

was only twenty years old when he attacked the crowd, and he is now a convicted murderer.<sup>4</sup> He is also a neo-Nazi.<sup>5</sup>

Organizers of “Unite the Right” advertised the rally as both a protest against the removal of a Robert E. Lee memorial and, more importantly, as an opportunity to unify splintered far-right and alt-right groups under a banner of white nationalism.<sup>6</sup> During the rally and demonstrations that followed, marchers carried paraphernalia adorned with extremist right-wing logos and repeatedly shouted slogans associated with Nazism and white

---

<sup>4</sup> *Id.* Fields was initially charged with second-degree murder, but prosecutor Joe Platania announced the upgraded charge after reviewing video evidence from both a nearby restaurant’s and the surveillance cameras of a Virginia State Police helicopter. Duggan, *Charge Upgraded*, *supra* note 1; Kaylee Hartung & Darran Simon, *Charge Upgraded Against Suspect in Charlottesville Rally Killing*, CNN (Dec. 15, 2017, 7:00 AM), <http://www.cnn.com/2017/12/14/us/charlottesville-james-alex-fields-court-appearance/index.html> [<https://perma.cc/G78E-3BRP>]. Whether the crash was premeditated and intentional was initially disputed, with many claiming Fields acted in a state of panic, but prosecutors claimed the footage shows Fields’ car stopping a block away from the protesters, reversing, then driving directly into the crowd before reversing and speeding away. Duggan, *Charge Upgraded*, *supra* note 1. Fields was ultimately convicted in state court of one count of first-degree murder, five counts of “aggravated malicious wounding,” and three counts of “malicious wounding,” and he faces additional counts in federal court. Paul Duggan, *James A. Fields Jr. Sentenced to Life in Prison in Charlottesville Car Attack*, WASH. POST (Dec. 11, 2018), [https://www.washingtonpost.com/local/public-safety/james-a-fields-jr-sentenced-to-life-in-prison-in-charlottesville-car-attack/2018/12/11/8b205a90-fcc8-11e8-ad40-cdf0e0dd65a\\_story.html](https://www.washingtonpost.com/local/public-safety/james-a-fields-jr-sentenced-to-life-in-prison-in-charlottesville-car-attack/2018/12/11/8b205a90-fcc8-11e8-ad40-cdf0e0dd65a_story.html) [<https://perma.cc/5XKZ-3KUB>]. Of the thirty-five people injured, eight were critically injured and suffered “permanent and significant physical impairment.” Duggan, *Charge Upgraded*, *supra* note 1.

<sup>5</sup> Abigail Hauslohner, Paul Duggan, Jack Gillum & Aaron C. Davis, *James Fields Jr.: A Neo-Nazi’s Violent, Rage-Fueled Journey to Charlottesville*, CHI. TRIB. (Aug. 18, 2017), <http://www.chicagotribune.com/news/nationworld/ct-james-fields-jr-charlottesville-20170818-story.html> [<https://perma.cc/HF4U-Z2P9?type=image>].

<sup>6</sup> Ryan M. Kelly, *Kessler Discusses KKK, Unite the Right Rallies and His Political Beliefs*, DAILY PROGRESS (Jul 11, 2017), [http://www.dailyprogress.com/news/local/kessler-discusses-kkk-unite-the-right-rallies-and-his-political/article\\_610ca84a-66a0-11e7-af48-1389a3205b81.html](http://www.dailyprogress.com/news/local/kessler-discusses-kkk-unite-the-right-rallies-and-his-political/article_610ca84a-66a0-11e7-af48-1389a3205b81.html) [<https://perma.cc/HB66-KTY7>]. The rally’s organizer, Jason Kessler, is an extremist right-wing blogger from Charlottesville and founder of white nationalist groups Unity and Security for America (also called “UniSecAmerica”), and The New Byzantium Project. *Id.*; Jason Kessler, S. POVERTY L. CTR., <https://www.splcenter.org/fighting-hate/extremist-files/individual/jason-kessler> [<https://perma.cc/MSL5-A4CY>]; Jason Kessler, *Announcing the New Byzantium Project*, PROTECT THE WEST (Sept. 24, 2017), <https://jasonkessler.us/2017/09/24/announcing-the-formation-new-byzantium> [<https://perma.cc/SM83-U55S>]. Like many far-right groups, UniSecAmerica describes its mission as “defending Western Civilization, including its history, culture, and peoples.” See UniSecAmerica, FACEBOOK, <https://www.facebook.com/pg/UniSecAmerica> [<https://perma.cc/BTF5-GKCE>]. Despite Kessler’s denial that he is a white supremacist, he is an avowed pro-white advocate and member of the white nationalist movement. See Kelly, *supra* note 6; Kessler *supra*. White nationalism is generally understood to be an umbrella term for white supremacist and white separatist ideology, and the Southern Poverty Law Center has classified Kessler as a white nationalist. See *White Nationalist*, S. POVERTY L. CTR., <https://www.splcenter.org/fighting-hate/extremist-files/ideology/white-nationalist> [<https://perma.cc/EA4Y-VEJC>]; Jason Kessler, *supra*.

nationalism.<sup>7</sup> Fields had traveled from his home in Ohio to attend the rally, participating in the protests and marching with the neo-Nazi group Vanguard America.<sup>8</sup> Though he made the journey by himself, as evidenced by the rapidly-growing white nationalist movement, he is not alone in his beliefs.<sup>9</sup>

The Charlottesville attack, motivated by extremism and formally described as domestic terrorism by the Department of Justice, may be a product of modern social unrest, but domestic terrorism itself is not a new phenomenon.<sup>10</sup> From the Ku Klux Klan to the Black Liberation Army to the Earth Liberation Front, extremist organizations that breed domestic terrorism have existed in the United States for decades.<sup>11</sup> Recently, however, these groups have seen a sharp uptick in activity.<sup>12</sup>

---

<sup>7</sup> *Deconstructing the Symbols and Slogans Spotted in Charlottesville*, WASH. POST (Aug. 18, 2017), <https://www.washingtonpost.com/graphics/2017/local/charlottesville-videos> [<https://perma.cc/HAC5-34WQ>].

<sup>8</sup> Hauslohner et al., *supra* note 5; see *Vanguard America*, ANTI-DEFAMATION LEAGUE, <https://www.adl.org/education/resources/backgrounders/vanguard-america> [<https://perma.cc/785K-R74K>] (discussing Vanguard America's increasing presence as a neo-Nazi extremist group). Although Vanguard America officially denies any affiliation with Fields, Fields was well-known in high school for espousing neo-Nazi views consistent with the group's mission. See Hauslohner et al., *supra* note 5 (interviewing Fields's former teacher about Fields's infatuation with Adolf Hitler and the Third Reich); Justin Moyer & Lindsey Bever, *Vanguard America, a White Supremacist Group, Denies Charlottesville Ramming Suspect Was a Member*, WASH. POST (Aug. 15, 2017), [https://www.washingtonpost.com/local/vanguard-america-a-white-supremacist-group-denies-charlottesville-attacker-was-a-member/2017/08/15/2ec897c6-810e-11e7-8072-73e1718c524d\\_story.html](https://www.washingtonpost.com/local/vanguard-america-a-white-supremacist-group-denies-charlottesville-attacker-was-a-member/2017/08/15/2ec897c6-810e-11e7-8072-73e1718c524d_story.html) [<https://perma.cc/W9Q2-CYHD>]. Vanguard America has denounced the attack, though Unite the Right rally organizer Jason Kessler maintains Fields' innocence. See Moyer & Bever, *supra*; Jason Kessler (@TheMadDimension), TWITTER, <https://web.archive.org/web/20180810224118/https://twitter.com/TheMadDimension/status/941453577981218816> [<https://perma.cc/J6DM-JNZP>].

<sup>9</sup> Duggan, *Charge Upgraded*, *supra* note 1; see Lauren Meltzer & Tony Dokoupil, *Hate Rising: White Supremacy's Rise in the U.S.*, CBS NEWS (Aug. 21, 2017, 5:57 PM), <https://www.cbsnews.com/news/hate-rising-cbsn-on-assignment> [<https://perma.cc/3SYG-2MK9>] (documenting the recent rise of white supremacy in the United States).

<sup>10</sup> Duggan, *Charge Upgraded*, *supra* note 1; Michael Edison Hayden, *Sessions Defends Trump's Comments on Charlottesville, Says Car Ramming Fits Definition of Domestic Terror*, ABC NEWS, (Aug. 14, 2017, 8:07 AM), <https://web.archive.org/web/20170829184136/http://abcnews.go.com/Politics/trumps-attorney-general-evil-charlottesville-car-ramming-fits/story?id=49202191> [<https://perma.cc/HN65-V8ZC>]; Joe Heim, *Recounting a Day of Rage, Hate, Violence and Death*, WASH. POST (Aug. 14, 2017), [https://www.washingtonpost.com/graphics/2017/local/charlottesville-time-line/?utm\\_term=.1420105843ac](https://www.washingtonpost.com/graphics/2017/local/charlottesville-time-line/?utm_term=.1420105843ac). [<https://perma.cc/G7D5-J3UK>]; see *infra* notes 11–12 and accompanying text (describing the origins of domestic terrorism).

<sup>11</sup> James F. Jarboe, Domestic Terrorism Section Chief, Counterterrorism Div., Fed. Bureau of Investigation, Address Before the House Resources Committee, Subcommittee on Forests and Forest Health (Feb. 12, 2002), <https://archives.fbi.gov/archives/news/testimony/the-threat-of-ecoterrorism> [<https://perma.cc/U73T-ZR5U>]; John W. Harris, Jr., *Domestic Terrorism in the 1980's*, 56 FBI L. ENFORCEMENT BULL. 5, 7 (1987); *Ku Klux Klan*, S. POVERTY L. CTR., <https://www.splcenter.org/fighting-hate/extremist-files/ideology/ku-klux-klan> [<https://perma.cc/REQ6-ABMC>].

<sup>12</sup> *Hate Map*, S. POVERTY L. CTR., <https://www.splcenter.org/hate-map> [<https://perma.cc/9F62-6DJW>].

In the last ten years, far-right violent attacks have skyrocketed, and between 1999 and 2017, the Southern Poverty Law Center reported an increase in the number of active hate groups from 457 to 954.<sup>13</sup> This outbreak is not restricted to the United States; the growing prominence of far-right political parties in Europe is well-documented, and in Britain, the number of suspected far-right extremists flagged for terror observation jumped thirty percent within the past year.<sup>14</sup>

While quantifying hate is not an easy task, numerous studies attribute this dramatic swell to the advent of the Internet and particularly to social media platforms.<sup>15</sup> The Internet is ubiquitous: in 2018, eighty-nine percent of Americans used the Internet, and approximately seven in ten had a social media profile or presence.<sup>16</sup> Part and parcel of that ubiquity, however, are tools that both facilitate easy communication for existing extremist operatives and accelerate self-radicalization among non-extremists.<sup>17</sup> In addition to the jihadi militant group ISIS's widely-publicized use of Twitter and YouTube as recruiting platforms, far-right- and far-left-wing extremist groups marinate in radicalizing echo chambers on Facebook, Twitter, Reddit, and similar websites, where they coordinate tactics and events.<sup>18</sup> The

<sup>13</sup> *Id.*; see Peter Bergen et al., *Part IV. What Is the Threat to the United States Today?*, NEW AMERICA, <https://www.newamerica.org/in-depth/terrorism-in-america/what-threat-united-states-today> [<https://perma.cc/LAY6-WGH9>]. Black separatist and far-left extremist groups have also seen increased activity, but violent acts are comparatively rare. Bergen et al., *supra*.

<sup>14</sup> See Lucy Pasha-Robinson, *Number of Far-Right Extremists Flagged to Government Terror Unit Soars 30% in a Year*, INDEPENDENT (June 19, 2017), <http://www.independent.co.uk/news/uk/home-news/finsbury-park-attack-far-right-extremist-rise-year-statistics-prevent-terrorism-scheme-referrals-a7798231.html> [<https://perma.cc/5HA3-FQF3>]; Amanda Taub, *What the Far Right's Rise May Mean for Germany's Future*, N.Y. TIMES (Sep. 26, 2017), <https://www.nytimes.com/2017/09/26/world/europe/germany-far-right-election.html> [<https://perma.cc/PT2G-QCPR>].

<sup>15</sup> See, e.g., Robin Thompson, *Radicalization and the Use of Social Media*, 4 J. STRATEGIC SECURITY 167, 168 (2012).

<sup>16</sup> Monica Anderson et al., *11% of Americans Don't Use the Internet. Who Are They?* (Mar. 5, 2018), PEW RESEARCH CTR., <http://www.pewresearch.org/fact-tank/2016/09/07/some-americans-dont-use-the-internet-who-are-they> [<https://perma.cc/8FVS-TQHH>] (noting further that of the 11% of Americans who do not use the Internet at all, most are seniors; only 2% of all Americans aged 18–29 do not use the Internet); *Social Media Fact Sheet*, PEW RESEARCH CTR. (Jan. 12, 2017), <http://www.pewinternet.org/fact-sheet/social-media> [<https://perma.cc/694U-R7WB>].

<sup>17</sup> See Thompson, *supra* note 15, at 171–72.

<sup>18</sup> See, e.g., J.M. BERGER, GEORGE WASHINGTON UNIV. PROGRAM ON EXTREMISM, NAZIS VS. ISIS ON TWITTER: A COMPARATIVE STUDY OF WHITE NATIONALIST AND ISIS ONLINE SOCIAL MEDIA NETWORKS 3–4, 21 (2016) (documenting a 600% increase in followers for right-wing extremists on Twitter between 2012 and 2016); *Hate on Social Media: A Look at Hate Groups and Their Twitter Presence*, SAFE HOME, <https://www.safehome.org/resources/hate-on-social-media> [<https://perma.cc/S57L-MRGB>] [hereinafter *Hate on Social Media*] (documenting the broad and growing presence of hate groups on Twitter since 2009, including the increase of average “likes” per post from 0.21 “likes” in 2012 to 7.68 “likes” in 2016); Christina Peneda, *What Does ISIS Post on YouTube?*, HOMELAND SECURITY DIGITAL LIBRARY (July 27, 2018) [<https://perma.cc/QSK3-4NXW>] (documenting ISIS's use of YouTube).

Charlottesville rally that James Fields attended was itself organized through both Facebook and privately hosted message boards.<sup>19</sup>

The Internet zeroes out information costs, allowing mass dissemination of what were once fringe ideologies by way of informational websites, discussion forums, and social media.<sup>20</sup> This cheap, easy, and often anonymous communication is the common denominator in extremist groups' abilities to organize and shepherd new members.<sup>21</sup> The facilitators of this easy communication are so-called "edge providers," meaning any entity on the Internet that provides content or services, such as social media and Internet message boards.<sup>22</sup> While far-right extremist content created by and for extremists can be found on their own niche websites like IronMarch.org or Stormfront.org, extremists also have significant (and rising) presence on social media.<sup>23</sup> Common social media platforms include well-known edge providers like YouTube, Facebook, and Twitter, but social media also encompasses

---

<sup>19</sup> Alex Heath, *Facebook Removed the Event Page for White Nationalist 'Unite the Right' Rally in Charlottesville One Day Before It Took Place*, BUS. INSIDER (Aug. 14, 2017, 5:36 PM), <http://www.businessinsider.com/facebook-removed-unite-the-right-charlottesville-rally-event-page-one-day-before-2017-8> [<https://perma.cc/FFE3-ZHVT>] (discussing Facebook's removal of the rally event page one day before the event itself); see Dara Kerr, *White Supremacist Parties? Airbnb Says Not in My House*, CNET (Aug. 9, 2017, 10:27 PM), <https://www.cnet.com/uk/news/airbnb-says-no-white-supremacist-parties-in-my-house> [<https://perma.cc/9LFN-TDDU?type=image>] (citing the forum of the now-defunct far-right website *The Daily Stormer*, which Unite the Right rally attendees used to organize transportation and lodging via Airbnb (<https://bbs.dailystormer.com/t/join-daily-stormer-staff-at-the-unite-the-right-rally-in-charlottesville-virginia/124489/68>)).

<sup>20</sup> Anne Stenersen, *The Internet: A Virtual Training Camp?* 20 TERRORISM & POL. VIOLENCE 215, 215–33 (2008); Thompson, *supra* note 15, at 168.

<sup>21</sup> Stenersen, *supra* note 20, at 215–33; Thompson, *supra* note 15, at 168.

<sup>22</sup> FCC Open Internet Order, 47 C.F.R. § 8.2(a) (2015) (defining edge provider as "[a]ny individual or entity that provides any content, application, or service over the Internet, and any individual or entity that provides a device used for accessing any content, application, or service over the Internet"); Thompson, *supra* note 15, at 171–72. "Edge providers" take their name from the layered architecture of the Internet. Annemarie Bridy, *Remediating Social Media: A Layer-Conscious Approach*, 24 B.U. J. SCI. & TECH. L. 193, 199 (2018). For regulation purposes, the Internet is comprised of two layers: physical infrastructure (such as broadband cable), and applications that run on the physical infrastructure (such as social media websites). *Id.* The physical infrastructure comprises the "core" of the network, carrying data between the applications and individuals at the "edges" of the network. *Id.*

<sup>23</sup> See, e.g., Berger, *supra* note 18; *Hate on Social Media*, *supra* note 18; *Welcome to Hate Planet*, IRON MARCH, <https://web.archive.org/web/20171106202658/http://ironmarch.org> [<https://perma.cc/EK29-EMT7>]; *Welcome to Stormfront*, STORMFRONT, <http://www.stormfront.org> [<https://perma.cc/QW48-6YLL>] (framing their mission as equivalent to other celebrations of minority culture). Stormfront, founded in 1995, is one of the oldest white supremacist websites and is today predominantly focused on recontextualizing white nationalism to seem more reasonable and thus more easily digestible to conservatives in mainstream politics. Priscilla Marie Meddaugh & Jack Kay, *Hate Speech or "Reasonable Racism?" The Other in Stormfront*, 24 J. MASS MEDIA ETHICS, 251, 251 (2009).

any application that enables users to network with one another.<sup>24</sup> Like any other Internet users, white supremacist groups use all forms of Internet communications.<sup>25</sup> White supremacists are certainly not the only extremists who use the Internet, but because the majority of domestic terror attacks within the past ten years have been committed by far-right extremists, this Note focuses on far-right ideology.<sup>26</sup>

Fields's attack amplified public consciousness of far right extremism and contributed to discourse about the interplay between the Internet and rapid radicalization, and what, if anything, the law should do about it.<sup>27</sup> In search of a cause for increasingly violent domestic terror attacks, critics of edge providers cite providers' perceived inability (or unwillingness) to curtail extremist and terrorist use of their platforms.<sup>28</sup> While some commentators advise that edge providers take internal action, like suspending and demoting extremist users' accounts, recent lawsuits, articles, and opinion pieces suggest another solution: hold the edge providers liable for providing support to domestic terrorists.<sup>29</sup> This advocacy follows current litigation

---

<sup>24</sup> *Social Media*, MERRIAM-WEBSTER (2018), <https://www.merriam-webster.com/dictionary/social%20media> [<https://perma.cc/SH77-UQHJ>]; Margaret Rouse, *Edge Provider*, WHATIS (Apr. 2017) <https://whatis.techtarget.com/definition/edge-provider> [<https://perma.cc/8N2R-G5S9>]; *supra* note 22 and accompanying text.

<sup>25</sup> See Berger, *supra* note 18 (documenting broad use of various Internet platforms by white supremacists).

<sup>26</sup> See SÉRAPHIN ALAVA ET AL., UNITED NATIONS EDUC., SCI., & CULTURAL ORG., YOUTH AND VIOLENT EXTREMISM ON SOCIAL MEDIA: MAPPING THE RESEARCH 23 (2017) <http://unesdoc.unesco.org/images/0026/002603/260382e.pdf> [<https://perma.cc/NN9T-VXUU>] (finding that Internet exposure to left-wing discourse does not, comparatively, have the same radicalizing effect as similar exposure to right-wing discourse); Alex Nowrasteh, *Terrorism Deaths by Ideology: Is Charlottesville an Anomaly?*, CATO INST. (Aug. 14, 2017) <https://www.cato.org/blog/terrorism-deaths-ideology-charlottesville-anomaly> [<https://perma.cc/5EN5-ZWM5>] (finding right-wing terrorism to have been nearly ten times deadlier than left-wing terrorism between 1992 and 2017).

<sup>27</sup> See, e.g., Daniel L. Byman, *Should We Treat Domestic Terrorists the Way We Treat ISIS?: What Works—and What Doesn't*, BROOKINGS INST. (Oct. 3, 2017) <https://www.brookings.edu/articles/should-we-treat-domestic-terrorists-the-way-we-treat-isis-what-works-and-what-doesnt> [<https://perma.cc/AA4C-W7VP>] (using Fields's attack as a lens to assess the benefits and consequences of expanding terrorism laws to include domestic terrorism, including any expansion's effect on Internet companies).

<sup>28</sup> See, e.g., Sam Levin, *James Damore, Google, and the YouTube Radicalization of Angry White Men*, THE GUARDIAN (Aug. 13, 2017), <https://www.theguardian.com/technology/2017/aug/13/james-damore-google-memo-youtube-white-men-radicalization> [<https://perma.cc/7K7M-8H8G>] (suggesting that YouTube algorithms that redirect viewers of political content to increasingly extreme content, some of it terroristic in nature, are responsible for radicalization, and criticizing YouTube for not adequately addressing the problem).

<sup>29</sup> E.g., Richard L. Hason, *Cheap Speech and What It Has Done (to American Democracy)*, 16 FIRST AM. L. REV. 200, 200 (2017) (arguing for re-examining the First Amendment and enacting regulation or legislation to hold social media companies legally accountable for "fake news" in the form of false political advertising); Arthur Chu, *Mr. Obama, Tear Down This Liability Shield*, TECHCRUNCH (Sep. 29, 2015) <https://beta.techcrunch.com/2015/09/29/mr-obama-tear-down-this-liability-shield> [<https://perma.cc/VY4D-C8SK>] (proposing the repeal of § 230 of the Communica-

trends in the foreign terror sphere, where several victims of international terror attacks have attempted to impose liability on various social media companies for allowing terrorists to use their platforms.<sup>30</sup>

Domestic terrorism poses a more difficult problem for any potential plaintiffs, as the legal framework for enforcing civil anti-terrorism law against homegrown terrorists is threadbare compared to its international counterpart.<sup>31</sup> Furthermore, any proponent of imposing liability on social media services or other edge providers for hosting domestic terrorism faces the same roadblock as plaintiffs in similar foreign terror suits: § 230 of the Communications Decency Act (“CDA”).<sup>32</sup> Section 230 eliminates the concept of vicarious publisher liability for edge providers.<sup>33</sup> Offline, publishers are liable for the speech of their users, but § 230 prohibits treating edge providers as the publishers of user-created content on their platforms.<sup>34</sup> Although seemingly unassailable in its current form, § 230 currently faces congressional challenges that may significantly erode its efficacy as a liability shield, which may give rise to lawsuits challenging the breadth of its protections.<sup>35</sup>

Part I of this Note outlines the federal framework for enforcing anti-terrorism statutes against domestic terrorists and for creating liability for parties who might provide material support to domestic terrorism, including

---

tions Decency Act (“CDA”) to allow private civil liability for social media companies whose platforms are used to facilitate harassment campaigns); *see infra* note 30 and accompanying text (describing the challenges to the breadth of the CDA, which otherwise barred the plaintiffs from suit against tech companies for allegedly supporting terrorism).

<sup>30</sup> *See, e.g.,* *Gonzalez v. Google, Inc.*, 282 F. Supp. 3d 1150, 1154–55 (N.D. Cal. 2017) (dismissing an attempt to hold Google liable for materially supporting terrorism where ISIS members posted harmful content on Google platforms); *Pennie v. Twitter, Inc.*, 281 F. Supp. 3d 874, 877 (N.D. Cal. 2017) (dismissing an attempt to hold Twitter liable for materially supporting terrorism by allowing DFOT group Hamas onto its platform, where American Micah Johnson was allegedly radicalized to shoot five Dallas police officers); *Cohen v. Facebook, Inc.*, 252 F. Supp. 3d 140, 146 (E.D.N.Y. 2017) (dismissing an attempt to hold Facebook liable for materially supporting terrorism by allowing Palestine-affiliated groups to “incite, enlist, organize, and dispatch would-be killers to ‘slaughter Jews’”).

<sup>31</sup> *See* 18 U.S.C. § 2333 (2012) (providing a civil remedy for victims of foreign terrorism, but not providing the same for victims of domestic terrorism); 18 U.S.C. § 2339A (functioning as the only law under which material support for domestic terrorism may be prosecuted); 18 U.S.C. § 2339B (permitting criminal prosecution for making donations to designated foreign terror organizations).

<sup>32</sup> *See* 47 U.S.C. § 230(c) (2012); *see, e.g., Gonzalez*, 282 F. Supp. 3d at 1167 (dismissed as barred by the CDA); *Pennie*, 281 F. Supp. 3d at 888 (same); *Cohen*, 252 F. Supp. 3d at 155 (same).

<sup>33</sup> 47 U.S.C. § 230(c); *Vicarious Liability*, BLACK’S LAW DICTIONARY (10th ed. 2014).

<sup>34</sup> 47 U.S.C. § 230(c).

<sup>35</sup> *See, e.g.,* Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. 115-164 § 3, 132 Stat. 1253, 1253–54 (creating an exception within § 230 for sex trafficking laws such that victims of sex trafficking may hold edge providers civilly liable as the publisher of unlawful content).

Internet edge providers.<sup>36</sup> Part II discusses how both the terrorism framework and § 230 prevent plaintiffs from holding edge providers liable for any contribution or provision of material support to domestic terrorist organizations or attacks.<sup>37</sup> Part III explores the consequences of allowing plaintiffs to hold edge providers liable for hosting terrorism-related content, ultimately proposing moderate alterations to federal terrorism law that leave § 230 intact.<sup>38</sup>

## I. THE LEGAL FRAMEWORK FOR DOMESTIC TERRORISM AND THIRD-PARTY LIABILITY

### A. Domestic Terrorism and Federal Law

A civil plaintiff attempting to sue any edge provider for hosting domestic terrorism faces not so much an uphill challenge as a ninety-degree hike up Mount Everest, and the first peak is finding a definition for “domestic terrorism.”<sup>39</sup> Unlike foreign terrorism, domestic terrorist activities are defined primarily by who carries them out, rather than by any organizations to which those individuals may belong.<sup>40</sup> This is because Congress’s statutory definitions provide means to categorize *foreign* terrorist organizations and prosecute them for acts of violence, but do not offer the same tools for domestic terrorism.<sup>41</sup> Instead, domestic terrorism is statutorily defined by the characteristics and context of individual violent activities—specifically, illegal dangerous acts conducted in the United States, with the intention of intimidating the public, and for the purposes of influencing policy.<sup>42</sup> Alt-

---

<sup>36</sup> See *infra* notes 39–99 and accompanying text.

<sup>37</sup> See *infra* notes 100–196 and accompanying text.

<sup>38</sup> See *infra* notes 197–251 and accompanying text.

<sup>39</sup> Compare 18 U.S.C. § 2331(5) (characterizing domestic terrorism broadly as violent acts committed with the intent to influence policy or intimidate the population), with FED. BUREAU OF INVESTIGATION, DOMESTIC TERRORISM IN THE POST-9/11 ERA (2009), [https://archives.fbi.gov/archives/news/stories/2009/september/domterror\\_090709](https://archives.fbi.gov/archives/news/stories/2009/september/domterror_090709) [<https://perma.cc/XW9L-GK9D>] (defining domestic terrorism as “Americans attacking Americans based on U.S.-based extremist ideologies”); see generally *infra* notes 40–60 and accompanying text.

<sup>40</sup> JEROME P. BJELOPERA, CONG. RESEARCH SERV., R44921, DOMESTIC TERRORISM: AN OVERVIEW 4 (2017); see *e.g.*, 18 U.S.C. §§ 2331, 2333, 2339A, 2339B (drawing consistent legal distinctions between domestic terror attacks and foreign terrorist organizations).

<sup>41</sup> BJELOPERA, *supra* note 40, at 4; see, *e.g.*, Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. 104-132 § 219, 110 Stat. 1214, 1248 (1996), 8 U.S.C. § 1189 (2012). Section 219 permits the Secretary of State to designate non-United-States-based extremist groups as Foreign Terrorist Organizations. 8 U.S.C. § 1189. Designating a group as a DFTO allows prosecutors access to DFTO-specific statutes such as § 2339B, and it also permits the Secretary of the Treasury to freeze the DFTO’s assets. *Id.*

<sup>42</sup> 18 U.S.C. § 2331(5) (prohibiting “acts dangerous to human life that are a violation of the criminal laws of the United States . . . [which] appear to be intended . . . to intimidate or coerce a civilian population . . . [in order] to influence the policy of a government by intimidation or coercion”). This section’s language tracks with the statutory definition of international terrorism, mi-

though U.S. law defines international terrorism in the same terms, U.S. policy generally regards domestic terrorism as “Americans attacking Americans based on U.S.-based extremist ideologies.”<sup>43</sup>

Federal law reflects this distinction between foreign terror organizations and domestic terror threats, creating wrinkles for prosecutors.<sup>44</sup> Unlike foreign terrorism, domestic terrorism is not actually a federal crime.<sup>45</sup> There is no specific statute under which domestic terrorism can be prosecuted, because, although Congress provided a definition for domestic terrorism in the PATRIOT Act at 18 U.S.C. § 2331(5), the criminal offenses in the Act are restricted to acts committed outside the United States against a U.S. national.<sup>46</sup> 18 U.S.C. § 2332b offers an enumerated list of federal crimes of terrorism, but it applies only to acts that transcend national boundaries.<sup>47</sup> In the absence of an actual statute for domestic terrorism, when prosecuting a domestic terrorist act, prosecutors may instead use enhancement provisions in the Federal Sentencing Guidelines.<sup>48</sup> These Guidelines apply when the underlying conduct involves the same actions as one of the enumerated terrorism crimes in § 2332(b) (excluding the international component), or if

---

nus the requirement that the act transcend national boundaries, and both statutes define terrorism through characterization of specific behaviors that ultimately constitute terrorism, rather than list a set of an enumerated offenses. Reuven Young, *Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation*, 29 B.C. INT’L & COMP. L. REV. 23, 27 (2006).

<sup>43</sup> FED. BUREAU OF INVESTIGATION, *supra* note 39. Compare 18 U.S.C. § 2331(1)(B), with 18 U.S.C. § 2331(5)(B) (defining, with identical language, what constitutes an actor’s intent to terrorize).

<sup>44</sup> Compare 18 U.S.C. § 2331(1)(B), with 18 U.S.C. § 2331(5)(B) (using identical language to define both domestic and international terrorism). A significant challenge posed by the threat-based nature of domestic terrorism prosecutions is the difficulty of distinguishing attacks rooted in ideology from hate crimes, which, while also driven by ideology, are acts of “personal malice” and do not fit the definition of domestic terrorism under § 2331(5). BJELOPERA, *supra* note 40, at 4. Because there is no criminal cause of action for domestic terrorism, terrorism is often prosecuted under hate crime statutes, further blurring the line between hate crimes and terrorism. See, e.g., *United States v. Harpham*, No. 2:11-CR-00042-JLQ, 2015 WL 4623717, \*1 (E.D. Wa. Aug. 3, 2015). Kevin Harpham pled guilty to hate crimes and attempted use of a weapon of mass destruction after he attempted to detonate a bomb during a Martin Luther King, Jr. parade in Spokane, Washington. *Id.* The attack was racially motivated, and authorities continuously characterized his actions as terrorism. *Id.* at \*3; Mark F. Giuliano, Assistant Dir., Counterterrorism Div., Fed. Bureau of Investigation, Speech at The Washington Institute for Near East Policy Stein Program on Counterterrorism and Intelligence (Apr. 14, 2011), <https://archives.fbi.gov/archives/news/speeches/the-post-9-11-fbi-the-bureaus-response-to-evolving-threats> [<https://perma.cc/FA63-3PDB>].

<sup>45</sup> See 18 U.S.C. § 2332b (requiring as an essential element that terrorist crimes be committed by a foreign national or in a foreign country); BJELOPERA, *supra* note 40, at 4.

<sup>46</sup> Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56 § 802(a)(4), 115 Stat. 272, 376 (2001), 18 U.S.C. § 2331(5); see 18 U.S.C. § 2332b (enumerating several crimes which share the core requirement that the act be committed either by a foreign national or in a foreign country).

<sup>47</sup> 18 U.S.C. § 2332b.

<sup>48</sup> U.S. SENTENCING COMM’N, GUIDELINES MANUAL § 3A1.4 (2016).

the conduct was intended to promote terrorism.<sup>49</sup> The Federal Bureau of Investigation (“FBI”) recognizes domestic terrorism but often declines to refer to actual attacks as such, in part because there is no domestic terror statute, but also because publication of such comments would be highly prejudicial in domestic courts.<sup>50</sup>

There is also no civil remedy for victims of domestic terrorism.<sup>51</sup> In 1992, Congress passed the Federal Courts Administration Act, adding § 2333 to Title 18 of the U.S. Code and creating a civil cause of action for U.S. nationals injured by *international* terrorism.<sup>52</sup> Section 2333 functions by permitting civil suits against defendants accused of violating any of several enumerated criminal anti-terrorism statutes.<sup>53</sup> The law’s passage was part of an omnibus effort to improve federal courts, including the addition of a remedy in a field of law where existing legal systems and jurisdiction are both inherently lacking, due to the complex and international nature of foreign terrorism.<sup>54</sup> Although foreign terror organizations themselves might always be out of reach, by creating liability along any part of the “causal chain” of terrorism, Congress sought to disrupt the flow of money by targeting the finances of its sponsors.<sup>55</sup>

---

<sup>49</sup> See *id.* (providing enhancements for crimes where the defendant’s actions constitute domestic terrorism); see, e.g., *United States v. Arnaout*, 431 F.3d 994, 1001–02 (7th Cir. 2005) (holding that the Sentencing Guidelines apply to a conviction when the underlying conduct was intended to promote a federal crime of terrorism); *United States v. Graham*, 275 F.3d 490, 516 (6th Cir. 2001) (applying a domestic terrorism sentencing enhancement for broad conspiracy to promote terrorism, even though the felony conviction itself was not a terrorism offense as enumerated by § 2332).

<sup>50</sup> Ryan J. Reilly, *There’s a Good Reason Feds Don’t Call White Guys Terrorists, Says DOJ Domestic Terror Chief*, HUFFINGTON POST (Jan. 1, 2018, 9:32 AM), [https://www.huffingtonpost.com/entry/white-terrorists-domestic-extremists\\_us\\_5a550158e4b003133ecceb74](https://www.huffingtonpost.com/entry/white-terrorists-domestic-extremists_us_5a550158e4b003133ecceb74) [<https://perma.cc/5ZXB-X77V>]. As federal prosecutors do not have a blanket statute criminalizing “domestic terrorism” under which to prosecute acts that otherwise fall under the § 2331(5) definition, the Department of Justice is hesitant to use the term “terrorism” in prosecution for fear that a judge might consider it prejudicial. *Id.*

<sup>51</sup> See 18 U.S.C. § 2333 (providing a civil remedy only for victims of foreign terrorism); *infra* notes 52–60 (discussing both the framework of civil remedies for foreign terrorism and the exclusion of domestic terrorism from that framework).

<sup>52</sup> Federal Courts Administration Act of 1992, § 1003, Pub. L. 102-572, 106 Stat. 4506, 4521 (1992).

<sup>53</sup> 18 U.S.C. § 2333.

<sup>54</sup> See S. REP. NO. 102-342, at 16, 22, 45 (1992) (justifying the creating of § 2333 when passing the Federal Courts Administration Act of 1992).

<sup>55</sup> *Id.* at 22. Congress expanded liability in 2016 by adding a provision which provides a cause of action against any person who conspires with anyone who commits an act of international terrorism. Justice Against Sponsors of Terrorism Act, Pub. L. 114-222 § 4, 130 Stat. 852, 854 (2016), 18 U.S.C. § 2333(d). The purpose of this expansion was to clarify that liability applies to anyone who directly *or* indirectly provides material assistance or support to foreign terror. Justice Against Sponsors of Terrorism Act § 2.

Congress unambiguously, explicitly excluded domestic terrorism from its § 2333 civil remedy, but even if it had not been excluded, applying § 2333 in domestic terrorism cases would be very difficult.<sup>56</sup> Section 2333 permits a litigant to use antiterrorism criminal statutes as private causes of action, but the vast majority of those statutes criminalize specific acts of *foreign* terrorism.<sup>57</sup> The only major criminal terrorism statute that does not require an international element is 18 U.S.C. § 2339A, which prohibits a third party from providing material support to a terror attack.<sup>58</sup> Theoretically, a plaintiff could file a civil action using § 2339A, but because § 2333 precludes that possibility, the only civil remedies available to victims of domestic terror attacks are traditional tort actions.<sup>59</sup> Domestic terrorism victims may commence any applicable tort action, such as wrongful death lawsuits, but they are not entitled to the special awards § 2333 confers (treble damages, costs, and attorney's fees).<sup>60</sup>

### *B. Third-Party Liability in the Terrorism Sphere*

Sections 2339A and 2339B of Title 18 both create third-party liability—i.e., liability for parties who provide material support, services, and resources to terrorists.<sup>61</sup> Although the two statutes were, respectively, substantially amended and first enacted in response to a domestic terror attack (the 1995 Oklahoma City bombing), the law once again distinguishes for-

---

<sup>56</sup> See 18 U.S.C. § 2333 (“Any national of the United States injured by . . . *international* terrorism . . . may sue therefor . . .”) (emphasis added); *supra* notes 44–49 and accompanying text (explaining that domestic terrorism is not itself a federal crime that can be prosecuted, and thus cannot be a civil cause of action).

<sup>57</sup> See, e.g., 18 U.S.C. § 2332b (creating specific penalties for killing, kidnapping, assaulting, etc., when conduct transcends national boundaries); *id.* § 2339B (prohibiting material support for foreign terror organizations).

<sup>58</sup> *Id.* § 2339A. Section 2339A does not exclude domestic terrorism, but is instead limited to a number of enumerated offenses, some of which have international components. *Id.* § 32 (prohibiting destruction of aircraft or aircraft facilities”), § 37 (prohibiting violence at international airports), § 175 (prohibiting use, possession, or transport of biological weapons), § 229 (prohibiting use, possession, or transfer of chemical weapons), § 1114 (prohibiting killing of federal employees), § 1116 (prohibiting killing of foreign officials), § 1361 (prohibiting damage to government property), § 1362 (prohibiting damage to communication infrastructure), § 1992 (prohibiting violence against mass transportation systems), § 2332f (prohibiting bombings of government, public, or infrastructure facilities).

<sup>59</sup> 18 U.S.C. § 2333; see e.g., Complaint, *Hurd v. United States*, No. 2:16-cv-02409 (D. S.C., July 1, 2016) (filing a wrongful death suit against the Federal Bureau of Investigation (FBI) for allowing Charleston church shooter Dylann Roof to obtain the firearm he used when committing mass murder).

<sup>60</sup> See 18 U.S.C. § 2333(a); S. REP. NO. 102-342 at 45; see, e.g., Complaint, *supra* note 59.

<sup>61</sup> 18 U.S.C. §§ 2339A, 2339B.

eign terror organizations from general terror threats, providing a more robust enforcement system against the former.<sup>62</sup>

Section 2339B prohibits knowingly providing support or resources to any designated foreign terrorist organization (“DFTO”).<sup>63</sup> Section 2339A, by contrast, is both broader and more narrow: narrowly, it criminalizes providing (or concealing the source of) material support or resources knowing those resources will be used to carry out an actual terror *attack* (as opposed to supporting an unrelated part of the organization), but more broadly, the support is criminal regardless of the attacker’s affiliation.<sup>64</sup> In essence, under § 2339A, a third party is criminally liable for providing material support to a domestic terrorist attack, but not to a domestic terrorist organization.<sup>65</sup>

Despite § 2339A’s origin in homegrown terrorism, third parties culpable under § 2339A for providing support to domestic attacks are rarely prosecuted as such.<sup>66</sup> Since the September 11th al-Qaeda attacks, the FBI has focused its domestic investigation efforts almost exclusively on self-radicalizing individuals associated with Islamic jihadi terrorism.<sup>67</sup> Of the forty-five cases the Department of Justice prosecuted under § 2339A be-

<sup>62</sup> See Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322 § 120005, 108 Stat. 1796, 2022 (1994); 18 U.S.C. §§ 2339A, 2339B. Section 2339A was initially passed as part of a broad crime bill unrelated to terrorism in 1994. Violent Crime Control and Law Enforcement Act § 120005. Less than a year later, motivated by U.S. right-wing extremism, Timothy McVeigh and Terry Nichols detonated a truck bomb in downtown Oklahoma City, killing 168 Americans in what remains the deadliest act of domestic terrorism in American history. Jo Thomas, *McVeigh Guilty on All Counts in the Oklahoma City Bombing; Jury to Weigh Death Penalty*, N.Y. TIMES (June 3, 1997), <http://www.nytimes.com/1997/06/03/us/mcveigh-guilty-all-counts-oklahoma-city-bombing-jury-weigh-death-penalty.html> [<https://perma.cc/8XLM-TZ7Q>]. In response, Congress passed the Antiterrorism and Effective Death Penalty Act (“AEDPA”) which amended § 2339A, added § 2339B, and added the Designated Foreign Terror Organization (“DFTO”) designation process. See Antiterrorism and Effective Death Penalty Act § 303; H.R. REP. NO. 104-383, at 37 (1995). Both sections were later strengthened and clarified by the USA PATRIOT Act, passed after the September 11th al-Qaeda attacks. USA PATRIOT Act § 215.

<sup>63</sup> 18 U.S.C. § 2339B(a)(1) (providing that “[w]hoever knowingly provides material support or resources to a foreign terrorist organization . . . shall be . . . imprisoned . . .,” with the limitation that such “a person must have knowledge that the organization is a designated terrorist organization”).

<sup>64</sup> *Id.* § 2339A(a) (“Whoever provides material support or resources . . . knowing or intending that they are to be used in preparation for . . . a violation of [enumerated offenses] shall be imprisoned . . .”). There are several dozen enumerated federal offenses considered terroristic in nature. See *id.*

<sup>65</sup> *Id.*

<sup>66</sup> See Scott Sullivan, *Prosecuting Domestic Terrorism as Terrorism*, JUST SECURITY (Aug. 18, 2017), <https://www.justsecurity.org/44274/prosecuting-domestic-terrorism-terrorism> [<https://perma.cc/4NF8-NDAJ>] (reporting only two federal prosecutions for material support of domestic terrorism between 2012 and 2017).

<sup>67</sup> *Id.*; see Giuliano, *supra* note 44 (characterizing homegrown Islamic radical extremism as one of the United States’ greatest domestic threats and one of the FBI’s top priorities).

tween 2012 and 2017, only two defendants were not sympathizers of transnational jihadi terror groups.<sup>68</sup>

The final distinction between domestic and international terror material support law is that there is no civil remedy for providing material support to domestic terrorists.<sup>69</sup> Section 2333 may permit bringing suit against violators of either § 2339A or § 2339B, but, as discussed above, § 2333 permits suits *only* for victims of international terrorism.<sup>70</sup> Absent any future congressional action, liable parties in domestic terror attacks may only be prosecuted by the government.<sup>71</sup> As these are criminal offenses, the government must prove every element, from knowledge to whether support is “material” to the underlying offense, beyond a reasonable doubt.<sup>72</sup>

To be convicted under § 2339A, a defendant must provide material support to a terrorist while knowing that it will be used to commit one of several offenses enumerated in the statute, and the perpetrator of the act itself must harbor ideology and motive such that it fulfills § 2331(5)’s definition of domestic terrorism.<sup>73</sup> Conspiring and attempting to provide support or resources is also a violation of § 2339A, as is concealing or disguising the origin or nature of support.<sup>74</sup> “Material support” for the felonies enumerated in both § 2339A and § 2339B includes the provision of property, services, facilities, personnel, equipment, or transportation.<sup>75</sup> Material

---

<sup>68</sup> Sullivan, *supra* note 66. Jihadi terrorism prosecutions did not always dominate the federal docket; before 2001, material support prosecutions in domestic terror cases were not uncommon. *See, e.g.*, David Johnston, *7 in Paramilitary Group Arrested in West Virginia*, N.Y. TIMES (Oct. 12, 1996), <http://www.nytimes.com/1996/10/12/us/7-in-paramilitary-group-arrested-in-west-virginia.html> [https://perma.cc/53H2-RERA] (reporting a material support prosecution against members of a white nationalist paramilitary group called the Mountaineer Militia); *Militia Head Jailed on Bomb Plot Charges*, L.A. TIMES (Dec 9, 1999), <http://articles.latimes.com/1999/dec/09/news/mn-42054> [https://perma.cc/GD56-WV8F] (reporting a material support prosecution against the leader of a white nationalist militia coalition called the Southeastern States Alliance).

<sup>69</sup> 18 U.S.C. §§ 2333, 2339A, 2339B; CHARLES DOYLE, CONGR. RESEARCH SERV., R41333, TERRORIST MATERIAL SUPPORT: AN OVERVIEW OF 18 U.S.C. § 2339A AND § 2339B, at 12 (2016), <https://fas.org/sgp/crs/natsec/R41333.pdf> [https://perma.cc/AC2G-MEMA].

<sup>70</sup> *See* DOYLE, *supra* note 69.

<sup>71</sup> *See* 18 U.S.C. § 2333; *id.* § 2339A.

<sup>72</sup> *Id.* § 2339A; *see In re Winship*, 397 U.S. 358, 361 (1970) (cementing the reasonable doubt standard in American criminal jurisprudence).

<sup>73</sup> 18 U.S.C. §§ 2331(5), 2339A.

<sup>74</sup> *Id.* § 2339A. The offenses enumerated in § 2339A include (1) destruction of aircraft or airports; (2) possession of biological or chemical weapons; (3) possession of plastic explosives; (4) perpetrating several forms of violence on federal lands, against federal property, or against federal officials acting in their capacities; (5) bombing places of public use or interstate commerce; and (6) sabotaging mass transportation or communication systems. *Id.* §§ 32, 37, 175, 229, 1114, 1116, 1361, 1362, 1992, 2332f.

<sup>75</sup> *Id.* §§ 2339A(b)(1), 2339B(g)(4). The full text of both sections defines material support as, “any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal sub-

support charges have rapidly become the most common vehicle for terrorism prosecutions, present in 69.4% of cases in 2010 (up from 11.6% in 2001).<sup>76</sup> As of 2017 material support is the most common charge in federal terrorism prosecutions.<sup>77</sup>

Unlike § 2339B, which has an express knowledge requirement, § 2339A does not expressly require a defendant to have known that the material support they provided would be used in a terrorist attack, only that the provided support *could* foreseeably be used in one.<sup>78</sup> Consequently, the knowledge requirement for material support is broader than that of § 2339B.<sup>79</sup> To be guilty under § 2339A, a defendant must have known that they provided material support to an actor, but needs only to be deliberately indifferent to, or have reckless disregard for, the consequences of that support.<sup>80</sup> In *Boim v. Holy Land Foundation*, the Seventh Circuit famously held that when a defendant donated funds to Hamas—a Palestinian political organization designated as a DFTO—despite the donation being earmarked for Hamas to perform educational outreach, Hamas’ use of those funds to kill an American national in an overseas terror attack was a reasonably foreseeable consequence of that donation, and the defendant was therefore criminally liable under § 2339A and civilly liable under § 2333.<sup>81</sup> Accordingly, it is typically sufficient for a plaintiff to prove that the defendant exhibited reckless disregard for the harm resulting from their provision of support, rather than actual knowledge of or intent to harm.<sup>82</sup>

---

stances, explosives, personnel . . . and transportation, except medicine or religious materials.” *Id.* §§ 2339A(b)(1), 2339B(g)(4).

<sup>76</sup> *CTR. ON LAW & SEC., N.Y. UNIV. SCHOOL OF LAW, TERRORIST TRIAL REPORT CARD: SEPTEMBER 11, 2001—SEPTEMBER 11, 2011*, at 21 (2011), <http://www.lawandsecurity.org/wp-content/uploads/2011/09/TTRC-Ten-Year-Issue.pdf> [<https://perma.cc/JK2F-PX3X>].

<sup>77</sup> *Domestic Terrorism Prosecutions Outnumber International*, TRAC REPORTS (Sept. 21, 2017) <http://trac.syr.edu/tracreports/crim/481> [<https://perma.cc/BL7S-YD7J>].

<sup>78</sup> *Compare* 18 U.S.C. § 2339A (lacking an express knowledge requirement), *with* 18 U.S.C. § 2339B (requiring express knowledge); *see* *Boim v. Holy Land Found.*, 549 F.3d 685, 691, 693–94 (7th Cir. 2008) (finding liability under § 2339A because the defendant’s donation being used to support a terrorist act was a reasonably foreseeable consequence of that donation, despite the defendant’s lack of knowledge or intent).

<sup>79</sup> *Boim*, 549 F.3d at 693–94 (finding liability under § 2339A because it was reasonably foreseeable that the defendant’s donation would be used to support a terrorist act). *Compare* 18 U.S.C. § 2339A, *with* 18 U.S.C. § 2339B.

<sup>80</sup> *Boim*, 549 F.3d at 693–94; *see also* *Holder v. Humanitarian Law Project*, 561 U.S. 1, 21–22 (2010) (holding that training members of a terrorist organization in peacekeeping still falls within the statute’s definition of “training” and is thus considered material support).

<sup>81</sup> *Boim*, 549 F.3d at 693–94; U.S. Dep’t of State, Office of the Coordinator for Counterterrorism, Designation of Foreign Terrorist Organizations, 62 Fed. Reg. 195, 52650 (Oct. 8, 1997), <https://www.gpo.gov/fdsys/pkg/FR-1997-10-08/pdf/97-27030.pdf> (designating Hamas as a DFTO).

<sup>82</sup> *See, e.g.*, *Gill v. Arab Bank*, 893 F. Supp. 2d, 474, 505–06 (E.D.N.Y. 2012) (holding, in agreement with the Seventh Circuit, that culpability under § 2339A does not require actual knowledge or intent).

When civil litigation is commenced under § 2339A, in addition to the requisite state of mind, a plaintiff must also prove that causation existed between a defendant's provision of material support and the instant harm.<sup>83</sup> The provision need not be the actual cause of an attack, but it must still be a proximate cause, meaning the harm must have been reasonably foreseeable.<sup>84</sup> In *Boim*, the court held that because it was foreseeable that the funds would go to terror activities and the contribution actually allowed Hamas to fund those activities, the plaintiff had established causation.<sup>85</sup> Both § 2339A and § 2339B contain this causation requirement, but litigation predicated on § 2339B fails more commonly on causation than § 2339A litigation.<sup>86</sup> Civil suits require an actual harm, proximately caused by the defendant's actions.<sup>87</sup> Proving that harm in § 2339B suits is more difficult because § 2339B expressly prohibits providing support to an *organization*, not a specific event.<sup>88</sup> A civil plaintiff alleging harm must therefore show that providing the organization with material support proximately caused the actual, specific harm.<sup>89</sup> By contrast, § 2339A concerns supporting a discrete act, which by nature of the allegation is less attenuated and thus more easily proven.<sup>90</sup>

The causation standards in § 2339A and § 2339B have proven themselves consistent roadblocks for plaintiffs attempting to hold edge providers liable for providing their platforms to terrorists.<sup>91</sup> There is, however, another substantial obstacle that has resulted in dismissal of almost every material support suit filed against edge providers: § 230 of the CDA.<sup>92</sup>

---

<sup>83</sup> *Boim*, 549 F.3d at 695–96.

<sup>84</sup> *Id.* at 697–98.

<sup>85</sup> *Id.* at 698.

<sup>86</sup> *See, e.g.*, *Fields v. Twitter, Inc. (Fields III)*, 881 F.3d 739, 749–50 (9th Cir. 2018) (dismissing a suit for lack of proximate cause between ISIS's use of Twitter generally and the actions of the person who perpetrated the attack but never himself made use of Twitter).

<sup>87</sup> *Id.* at 748.

<sup>88</sup> *Id.*

<sup>89</sup> *Id.*

<sup>90</sup> *See, e.g.*, *United States v. Stewart*, 590 F.3d 93, 99 (2d Cir. 2009) (upholding the material support conviction of an attorney for passing along a message directly connected to a terrorist act). In *Stewart*, the court upheld the § 2339A conviction of Lynne Stewart, an ex-attorney who had helped her then-client Omar Abdel-Rahman, a perpetrator of the 1993 World Trade Center bombings, pass along messages from prison. *Id.* at 99, 101. Rahman's supporters had asked for his advice on whether to ignore a ceasefire with the Egyptian government and resume violence, and Stewart passed along a message that he had "no objection" to ignoring the ceasefire. *Id.* at 99, 107.

<sup>91</sup> *See, e.g.*, *Gonzalez*, 282 F. Supp. 3d 1150 (dismissed for lack of causation); *Pennie*, 281 F. Supp. 3d at 874 (same); *Cohen*, 252 F. Supp. 3d 140 (same).

<sup>92</sup> *See* Eric Goldman, *Seventh Different Lawsuit Against Social Media Providers for "Material Support to Terrorists" Fails—Taamneh v. Twitter, TECH. & MARKETING L. BLOG* (Oct. 31, 2018) <https://blog.ericgoldman.org/archives/2018/10/seventh-different-lawsuit-against-social-media-providers-for-material-support-for-terrorists-fails-taamneh-v-twitter.htm> [<https://perma.cc/FFU9-XPNB>] [hereinafter Goldman, *Seventh Lawsuit*]; *infra* notes 93–99 and accompanying text.

*C. Section 230 of the Communications Decency Act*

Congress passed Section 230 as part of Title V of the 1996 Telecommunications Act.<sup>93</sup> Title V, also known as the Communications Decency Act, was an indecency and obscenity law intended to regulate online pornography.<sup>94</sup> While the Supreme Court eventually struck down the majority of the CDA as an unconstitutional violation of the First Amendment, § 230 survived.<sup>95</sup>

Section 230 prohibits plaintiffs from treating “provider[s] . . . of an interactive computer service” as publishers or speakers of content that is produced by someone else but hosted on the provider’s platform.<sup>96</sup> This prohibition encompasses both edge providers like Google and Facebook as well as Internet service providers (ISPs) that provide broadband or other comparable access to the Internet.<sup>97</sup> The CDA’s reach is broad, and that breadth has survived challenges ranging from failure of an ISP to provide a nondiscriminatory place of public accommodation, to trademark claims of unfair competition, and, most relevantly, to tort claims.<sup>98</sup> The CDA does not apply

---

<sup>93</sup> Telecommunications Act of 1996, Pub. L. No. 104-104 § 509, 110 Stat. 56, 137–39 (1996), 47 U.S.C. § 230(c) (2012).

<sup>94</sup> *Id.*

<sup>95</sup> See *Reno v. ACLU*, 521 U.S. 844, 874 (1997) (finding the majority of the Act to be an impermissible content-based restriction on speech, but finding § 230 content neutral and thus leaving it intact).

<sup>96</sup> 47 U.S.C. § 230(c)(1).

<sup>97</sup> *Id.*; see, e.g., *Caraccioli v. Facebook, Inc.*, 167 F. Supp. 3d 1056, 1066 (N.D. Cal. 2016) (holding that Facebook fits the definition of an “interactive computer service” and is therefore immune under § 230 from suits stemming from content on the Facebook platform); *Goddard v. Google, Inc.*, 640 F. Supp. 2d 1193 (N.D. Cal. 2009) (holding that the plaintiff’s claim that Google supported fraudulent advertising was barred by the CDA); *Noah v. AOL Time Warner, Inc.*, 261 F. Supp. 2d 532 (E.D. Va. 2003) (holding that TimeWarner Cable also fits the statutory definition and is similarly immune from suit).

<sup>98</sup> See *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102 (9th Cir. 2007) (finding immunity for edge provider CCBill in a trademark claim); *Saponaro v. Grindr, LLC*, 93 F. Supp. 3d 319 (D. N.J. 2015) (finding immunity for an edge provider Grindr in tort suit); *Noah*, 261 F. Supp. 2d at 532 (finding immunity for TimeWarner in nondiscrimination suit). In *Saponaro*, the court found that the CDA barred a negligence suit against online dating app Grindr for allegedly permitting a thirteen-year-old minor to misrepresent his age. 93 F. Supp. 3d at 321. Allegedly believing the underage user was of consenting age, the plaintiff had organized and performed a “threesome” with him. Police subsequently arrested the plaintiff and charged him with sexual assault. *Id.* In *Perfect 10*, the court dismissed the plaintiff’s trademark and unfair competition claims as barred by the CDA. 488 F.3d at 1108. The plaintiff, Perfect 10, published an adult entertainment magazine and operated a parallel subscription-based online service, the content of which was often pirated by rival subscription services. *Id.* CCBill, the defendant, is an online payment service that allows customers to pay for, among other things, online subscriptions. *Id.* Perfect 10 alleged that the webmasters with whom CCBill contracted had pirated their content, and by failing to monitor the services, CCBill was liable for violating Perfect 10’s trademarks. *Id.* In *Noah*, the court held that broadband ISP AOL TimeWarner was immune from a suit alleging discrimination. 261 F. Supp. at 534. The plaintiff, a Muslim, claimed that AOL violated his right to a nondiscriminatory place of public accommodation by permitting users to post harassing messages in its chatrooms.

to criminal law or enforcement, and thus the government may prosecute a computer service as the publisher of its content.<sup>99</sup>

## II. OBSTACLES TO IMPOSING LIABILITY ON THIRD PARTIES

Domestic terrorism is indisputably a problem in the United States, and while national attention focuses predominantly on radical Islamist terror, far-right white supremacist and anti-government terror attacks are no less common than those perpetrated by jihadists.<sup>100</sup> Between 2001 and 2015, right-wing extremists carried out nineteen lethal attacks and killed twice as many people as Muslim extremists, who only carried out seven lethal attacks.<sup>101</sup> Groups that radicalize attackers are also becoming more common; the Southern Poverty Law Center reports an increase in active hate groups from 457 in 1999 to 917 in 2016.<sup>102</sup> This rise is attributable at least in part to the advent of the Internet and of social media, which has enabled the flourishing of echo chambers accessible to anyone worldwide with a broadband connection.<sup>103</sup>

---

*Id.* The respective courts dismissed them all. *Perfect 10*, 488 F.3d at 1102; *Saponaro*, 93 F. Supp. 3d at 319; *Noah*, 261 F. Supp. 2d at 532.

<sup>99</sup> 47 U.S.C. § 230(e)(1) (distinguishing civil liability from criminal liability and stating that the statute shall have no effect on any federal criminal statute).

<sup>100</sup> Bergen et al., *supra* note 13.

<sup>101</sup> *Id.* This survey found that jihadists were responsible for the deaths of twenty-six people during this same time period, while right-wing extremists killed forty-eight. *Id.* The survey excluded any attacks that were not clearly tied to ideology. *Id.* This survey also predates the 2015 San Bernardino shooting and 2017 Pulse nightclub shooting, both perpetrated by self-proclaimed jihadists. See Alan Blinder, Frances Robles & Richard Pérez-Peña, *Omar Mateen Posted to Facebook Amid Orlando Attack, Lawmaker Says*, N.Y. TIMES (June 16, 2016), <https://www.nytimes.com/2016/06/17/us/orlando-shooting.html> [<https://perma.cc/4XNG-FP3N>] (reporting that Pulse nightclub shooter Omar Mateen had sworn allegiance to the Islamic State before and during the attack); Pete Williams & Halimah Abdullah, *FBI: San Bernardino Shooters Radicalized Before They Met*, NBC NEWS (Dec. 9, 2015, 1:42 PM) <https://www.nbcnews.com/storyline/san-bernardino-shooting/fbi-san-bernardino-shooters-radicalized-they-met-n476971> [<https://perma.cc/AD8H-KWXD>] (reporting on then-FBI Director James Comey's testimony that both San Bernardino shooters had self-radicalized in 2013).

<sup>102</sup> *Hate Map*, *supra* note 12; see Bergen et al., *supra* note 13. Black separatist and far-left extremist groups have also increased their activity, but violent acts are comparatively rare. See Bergen et al., *supra* note 13 (documenting the sharp rise of far-right deadly attacks between 2000 and 2018).

<sup>103</sup> See, e.g., INES VON BEHR ET AL., RAND CORP. EUROPE, RADICALISATION IN THE DIGITAL ERA: THE USE OF THE INTERNET IN 15 CASES OF TERRORISM AND EXTREMISM 17 (2013) [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR400/RR453/RAND\\_RR453.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf) [<https://perma.cc/A2P7-24CS>] (concluding that the Internet provides greater opportunities for radicalization and, while not the sole cause, acts as an “accelerant” in the process); Kieron O’Hara & David Stevens, *Echo Chambers and Online Radicalism: Assessing the Internet’s Complicity in Violent Extremism*, 7 POL’Y & INTERNET 4, 401, 402–03 (2015) (evaluating the harm—or lack thereof—of Internet echo chambers, given their pervasiveness); Thompson, *supra* note 15, at 168 (studying the impact of social media in particular on the radicalization process).

Given the considerable increase in both active hate groups and ideologically motivated violence over the past twenty years, it is not surprising that social and legal scholars are in search of solutions.<sup>104</sup> As the Internet has been instrumental in radicalization, it is also not surprising that proposed solutions sometimes center around platforms that host extremist and terrorist content, from large edge providers like Twitter to domain name registration services like GoDaddy.<sup>105</sup> Several terror victims have filed suits against Twitter, Facebook, and Google, attempting to actualize calls to hold tech companies responsible for the user speech on their platforms.<sup>106</sup> Thus far, this has not proven a fruitful endeavor.<sup>107</sup>

This Section explores the challenges of prosecuting or litigating domestic terror within the current legal framework.<sup>108</sup> Part A discusses how, even without the CDA, federal terrorism law precludes imposing liability on edge providers who would provide material support to acts of domestic terrorism.<sup>109</sup> Part B explores § 230 of the CDA in greater detail, including the immunities it confers to edge providers, dismissed and pending lawsuits attacking it, and current legislative threats to its existence.<sup>110</sup>

---

<sup>104</sup> See *Hate Map*, *supra* note 12; Bergen et al., *supra* note 13 (detailing the increase in hate groups and hate-motivated violence); see, e.g., Anti-Semitism Awareness Act of 2016, S.10, 114th Cong. § 4 (2016) (proposing a bill that would expand the Civil Rights Act of 1964 to include anti-Semitism and therefore expand the breadth of speech that can precipitate a civil rights investigation); Suzanne Nossel, *The Problem with Making Hate Speech Illegal*, FOREIGN POLICY (Aug. 14, 2017, 2:00 PM), <http://foreignpolicy.com/2017/08/14/the-problem-with-making-hate-speech-illegal-trump-charlottesville-virginia-nazi-white-nationalist-supremacist> [<https://perma.cc/MT25-QTA7>] (arguing that outlawing hate speech is not an appropriate legal solution).

<sup>105</sup> See, e.g., Byman, *supra* note 27 (discussing GoDaddy's history of providing domain names for white nationalist content); Noah Kulwin, *Twitter Is Still Trying and Failing to Solve Its White Supremacy Problem*, VICE NEWS (Nov. 16, 2017), [https://news.vice.com/en\\_us/article/gydda7/twitter-is-still-trying-and-failing-to-solve-its-white-supremacy-problem](https://news.vice.com/en_us/article/gydda7/twitter-is-still-trying-and-failing-to-solve-its-white-supremacy-problem) [<https://perma.cc/Q499-QZJ8>] (documenting and criticizing Twitter's failure to remove white supremacists from its platform); Heather Stewart & Jessica Elgot, *May Calls on Social Media Giants to Do More to Tackle Terrorism*, THE GUARDIAN, (Jan. 24, 2018), <https://www.theguardian.com/business/2018/jan/24/theresa-may-calls-on-social-media-giants-to-do-more-to-tackle-terrorism> [<https://perma.cc/UTA2-7KHE>] (reporting on British Prime Minister Theresa May's request for shareholders to pressure social media companies to combat terrorism).

<sup>106</sup> See, e.g., *Gonzalez v. Google, Inc.*, 282 F. Supp. 3d 1150 (N.D. Cal. 2017); *Pennie v. Twitter, Inc.*, 281 F. Supp. 3d 874, (N.D. Cal. 2017); *Cohen v. Facebook, Inc.*, 252 F. Supp. 3d 140 (E.D.N.Y. 2017) (dismissing all as barred under the CDA).

<sup>107</sup> Demetrick Pennie, *Section 230 of the CDA Must Align with the 21st Century*, LAW360 (July 26, 2017, 12:40pm) <https://www.law360.com/articles/947856/section-230-of-the-cda-must-align-with-the-21st-century> [<https://perma.cc/2EAN-DEPT>] (encouraging limiting legal roadblocks to open social media companies up to liability in response to domestic terror attacks).

<sup>108</sup> See *infra* notes 111–196 and accompanying text.

<sup>109</sup> See *infra* notes 111–143 and accompanying text.

<sup>110</sup> See *infra* notes 144–196 and accompanying text.

### A. Structural Limitations to Prosecuting Domestic Terrorism

The first obstacle to any kind of anti-terrorism enforcement is that no federal agency has wholesale regulatory authority over companies that provide platforms for user content.<sup>111</sup> While the Federal Communications Commission (“FCC”) regulates broadcast, its authority over the Internet extends only to network service providers (such as Comcast)—and that authority is ancillary at best.<sup>112</sup> The FCC cannot provide civil remedies, nor can it mandate that service providers turn over account information to law enforcement agencies or shut down accounts or websites.<sup>113</sup> Edge providers like social media websites fall under the purview of the Federal Trade Commission (“FTC”), whose jurisdiction over the Internet extends only to consumer protection, not content regulation.<sup>114</sup>

In the absence of regulatory authority or congressional action, an alternative means of moderating terrorist content on the Internet may lie in the courtroom.<sup>115</sup> The construction of terror laws, however, leaves little room for even prosecution of domestic terrorists themselves, much less any third party who may have provided material support to a domestic terrorist.<sup>116</sup>

The first crime to be pursued as an act of domestic terror under Attorney General Jefferson Sessions’s Department of Justice occurred on January 17th, 2018, when Taylor Michael Wilson was indicted on domestic terrorism charges for hijacking and attempting to crash an Amtrak train.<sup>117</sup> Wil-

<sup>111</sup> See John Eggerton, *Lax FTC Edge Enforcement Has Left ‘Gaping’ Hole*, BROADCASTING CABLE (May 7, 2018) <https://www.broadcastingcable.com/news/netcompetition-lax-ftc-edge-enforcement-left-gaping-hole> [<https://perma.cc/6SUR-BTTQ>] (discussing various federal agencies’ limited jurisdiction over content on the Internet).

<sup>112</sup> Restoring Internet Freedom, 83 Fed. Reg. 7852 (Feb. 22, 2018) (codified at 47 C.F.R. § 8, 20) (2019) (ordering the reclassification of the Internet to a Title I information service, stripping the Federal Communications Commission (“FCC”) of most regulatory authority in favor of a light-touch framework); Mario Trujillo, *FCC Says It Can’t Shut Down ISIS Websites*, THE HILL (Nov. 17, 2015), <http://thehill.com/policy/technology/260438-fcc-says-it-cant-shutdown-online-terrorist-activity> [<https://perma.cc/2KTF-XKDH>]; see also *F.C.C. v. Pacifica Found.*, 438 U.S. 726, 733–34 (1978) (upholding the FCC’s authority to promulgate indecency regulations for broadcast television). In a congressional hearing, former FCC chairman Tom Wheeler expressed both belief that the FCC did not have jurisdiction to target individual websites, and also disinterest in pursuing it. Trujillo, *supra*.

<sup>113</sup> Trujillo, *supra* note 112.

<sup>114</sup> Eggerton, *supra* note 111; see, e.g., Children’s Online Privacy and Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681–728 (authorizing the FTC to promulgate and enforce rules limiting websites from collecting data of children under thirteen).

<sup>115</sup> See, e.g., *Crosby v. Twitter, Inc.*, 303 F. Supp. 3d 564, 570 (E.D. Mich. 2018) (attempting to hold Twitter liable for hosting terrorism).

<sup>116</sup> See, e.g., 18 U.S.C. § 2339B (2012) (criminalizing providing material support to DFTOs).

<sup>117</sup> Complaint, *United States v. Wilson*, No. 4:18-cr-03005, 1 (D. Neb. 2018); see 18 U.S.C. § 1992 (criminalizing terrorist attacks against railroads or other mass transportation carriers); Eric Levenson, *Neo-Nazi Charged with Terrorism in Attempt to Wreck Amtrak Train, Complaint Says*, CNN (Jan. 17, 2017, 6:54 PM), <https://www.cnn.com/2018/01/09/us/nazi-white-supremacist-amtrak->

son, who had previously participated in the Charlottesville rally, boarded an Amtrak train with a fully loaded revolver on October 22nd, 2017, and triggered an emergency stop, allegedly intending to harm the passengers.<sup>118</sup> During his arrest, not only did the police who searched him uncover a gas mask, a knife, ammunition, and several speed loaders for the revolver, police also discovered that Wilson was carrying business cards for the National Socialist Movement (“NSM”), a neo-Nazi organization.<sup>119</sup> During the investigation, Wilson’s cousin informed police that Wilson had inadvertently connected with the NSM when researching forums online.<sup>120</sup>

If the NSM were classified as a DFTO and Wilson was a member of the NSM, any victim of Wilson’s violence would have a civil cause of action under 18 U.S.C. § 2333 against anyone who provided material support to the NSM as a whole, not just against Wilson himself.<sup>121</sup> But because the NSM is a domestic hate group, victims of the attack cannot pursue any claims against supporters of the NSM, and they must restrict all claims to third parties who supported Wilson directly.<sup>122</sup> The government has similarly limited recourse, restricted to prosecuting only Wilson himself (or supporters specifically of Wilson) for his specific enumerated offenses—in this case, hijacking a train—instead of the broader category of people who support the NSM as a whole.<sup>123</sup>

Attaching civil liability to third parties for providing material support to domestic terrorists is not possible by statute, but criminally prosecuting third parties for providing material support to domestic terrorists is, although possible, not much easier.<sup>124</sup> Unlike 18 U.S.C. § 2339B, which establishes criminal liability for supporting foreign terror organizations, 18 U.S.C. § 2339A—the only law establishing liability against domestic terrorists—applies only to parties who provide support for an actual act of ter-

---

terrorism-arrest-trnd/index.html [https://perma.cc/HJ83-3LLK] (confirming that Wilson was in attendance at Unite the Right).

<sup>118</sup> Complaint, *supra* note 117, at 10; Levenson, *supra* note 117.

<sup>119</sup> Levenson, *supra* note 117.

<sup>120</sup> *Id.*

<sup>121</sup> See 18 U.S.C. §§ 2333(d)(2), 2339B(a)(1) (“Whoever knowingly provides material support or resources to a *foreign terrorist organization* . . . shall be . . . imprisoned . . .”) (emphasis added). Of course, any plaintiff would still have to prove a causal nexus between the defendant’s support of the NSM and the harm of the attack. *Boim v. Holy Land Found.*, 549 F.3d 685, 691, 693–94 (7th Cir. 2008).

<sup>122</sup> See 18 U.S.C. § 2333.

<sup>123</sup> See *id.* §§ 2331(5), 2332B.

<sup>124</sup> See *id.* § 2339A (criminalizing providing material support to a terrorist act, not excluding domestic terrorist acts); 47 U.S.C. § 230 (barring holding a computer service liable as the speaker for the content it publishes, but creating an exception for criminal prosecutions); *infra* notes 125–135 and accompanying text.

ror.<sup>125</sup> The CDA notwithstanding, edge providers who knowingly and intentionally host members of DFTOs on their platforms could theoretically be held liable for materially supporting them under § 2339B, but if the organization is homegrown, providers evade liability.<sup>126</sup>

One example of a third party whose provision of a platform would otherwise constitute providing support to terrorist organizations (as opposed to a terrorist attack) is IronMarch.org.<sup>127</sup> Vanguard America, the organization with which James Fields marched in Charlottesville, traces its roots to IronMarch.org.<sup>128</sup> IronMarch.org is a message board that has spawned a number of far-right white supremacist groups, including “Atomwaffen Division,” a fascist paramilitary neo-Nazi organization.<sup>129</sup> Atomwaffen was founded in 2015 and announced its creation on IronMarch.org, but most

<sup>125</sup> 18 U.S.C. §§ 2339A, 2339B; *see* BJELOPERA, *supra* note 40, at 57–58 (explaining that there are no specific terrorism statutes under which domestic terrorists can be prosecuted—with the exception of § 2339A).

<sup>126</sup> *Compare* 18 U.S.C. § 2339A(a) (“Whoever provides material support or resources . . . knowing or intending that they are to be used in preparation for . . . a violation of [enumerated offenses] shall be imprisoned . . .”), *with* 18 U.S.C. § 2339B(a)(1) (providing for the imprisonment of anyone who “knowingly provides material support or resources to a foreign terrorist organization,” but requiring that the “person must have knowledge that the organization is a designated terrorist organization”).

<sup>127</sup> *See Welcome to Hate Planet*, *supra* note 23 (providing forum space targeted to paramilitary organizations like Atomwaffen, whose members perpetrated several violent attacks on Americans); *infra* notes 129–135 (describing the terrorist nature of Atomwaffen and the crimes committed by Atomwaffen members). The IronMarch.org website was recently taken down for unverifiable reasons by its owner, neo-Nazi Alisher Mukhitdinov, who was allegedly romantically involved with an Illinois woman who was arrested in 2015 for planning to commit a mass shooting in Nova Scotia. *Fascist Forge: A New Forum for Hate*, ANTI-DEFAMATION LEAGUE NEVADA (Jan. 15, 2019) <https://lasvegas.adl.org/fascist-forge-a-new-forum-for-hate> [<http://perma.cc/QR99-MWT8?type=image>]; *Illinois Woman with Neo-Nazi Leanings Charged in Canadian Mass Murder Plot*, S. POVERTY L. CTR. (Feb. 18, 2015), <https://www.splcenter.org/hatewatch/2015/02/18/illinois-woman-neo-nazi-leanings-charged-canadian-mass-murder-plot> [<https://perma.cc/G4HT-VK2U>] (citing Artard, *Lindsay Kantha Souvannarath / Heretics on Holiday - Failed Halifax Mass Shooter & Asian Nazi Fetishist*, KIWI FARMS (Feb. 14, 2015), <https://kiwifarms.net/threads/lindsay-kantha-souvannarath-heretics-on-holiday.7744/page-2> [<https://perma.cc/G5NE-NBK8>]) [hereinafter *Illinois Woman*]. She and her two co-conspirators all made use of Nazi iconography in their social media posts. *Illinois Woman*, *supra*.

<sup>128</sup> *Meet ‘Patriot Front’: Neo-Nazi Network Aims to Blur Lines with Militiamen, the Alt-Right*, S. POVERTY L. CTR., (Dec. 12, 2017), <https://www.splcenter.org/hatewatch/2017/12/11/meet-patriot-front-neo-nazi-network-aims-blur-lines-militiamen-alt-right> [<https://perma.cc/F3US-Y33K>] (hereinafter *Meet Patriot Front*).

<sup>129</sup> *Meet Patriot Front*, *supra* note 128. Unlike many far-right extremist organizations, Atomwaffen actively embraces Nazi iconography and fascist rhetoric. A.C. Thompson et al., *California Murder Suspect Said to Have Trained with Extremist Hate Group*, PROPUBLICA (Jan. 26, 2018, 7:46 PM) <https://www.propublica.org/article/california-murder-suspect-atomwaffen-division-extremist-hate-group> [<https://perma.cc/8TRM-D85T>]. The organization deliberately brands itself with Third Reich imagery, and members have posted videos online of themselves burning the Constitution and American flag. *Id.* Members also attend paramilitary training camps where they are trained in survival skills, firearms, and hand-to-hand combat. *Id.*

recently came to prominence in May of 2017 when Brandon Russell, one of its members, was arrested in Tampa, Florida after his roommate, Devon Arthurs, shot and killed their other two roommates.<sup>130</sup> All four of them were also Atomwaffen members.<sup>131</sup> Russell himself was found in possession of highly explosive compounds after police detected radioactivity in the apartment and he was accused by Arthurs of plotting to destroy electric power lines in South Florida and detonate explosive devices at a Miami nuclear power plant.<sup>132</sup>

Destruction of energy facilities, possession of nuclear material, and possession of chemical explosives are three of the enumerated offenses covered by § 2339A and § 2339B.<sup>133</sup> Were Atomwaffen a DFTO, and thus under the purview of § 2339B, IronMarch.org, which actively courted neo-Nazi violent fascism, would likely be liable for providing them with material support.<sup>134</sup> Section 2339A, on the other hand, would only permit liability

<sup>130</sup> Thompson et al., *supra* note 129; Adam Thorp, *Militant Neo-Nazi Group Claims Credit for Hanging Hitler Portrait, Swastikas on Campus Building*, CHI. MAROON (Dec. 5, 2016, 6:15 PM) <https://www.chicagomaroon.com/article/2016/12/6/militant-neo-nazi-group-claims-credit-hanging-hitl> [<https://perma.cc/EB9C-G8DX>].

<sup>131</sup> Niraj Chokshi, *Neo-Nazi Leader in Florida Sentenced to 5 Years Over Homemade Explosives*, N.Y. TIMES, Jan. 10, 2018, <https://www.nytimes.com/2018/01/10/us/brandon-russell-sentenced-neo-nazi.html> [<https://perma.cc/T4NK-U3YL>]; Thompson et al., *supra* note 129. Atomwaffen made news even more recently when member Samuel Woodward was charged in California with the murder of Blaze Bernstein, a student at the University of Pennsylvania. *See* Thompson et al., *supra* note 129. The prosecution is ongoing, but Woodward has been photographed and identified with Atomwaffen members and has engaged in guerilla training since 2016. *Id.* In his social media accounts, he describes himself as a National Socialist. *Id.* Bernstein, the victim, was gay and Jewish, and prosecutors are treating the murder as a hate crime. *Id.*

<sup>132</sup> Chokshi, *supra* note 131; Dan Sullivan, *National Guard 'Neo-Nazi' Aimed to Hit Miami Nuclear Plant, Roommate Says*, TAMPA BAY TIMES (June 13, 2017), <http://www.tampabay.com/news/courts/criminal/judge-sets-release-conditions-for-neo-nazi-in-tampa-palms-explosives-case/2327088> [<https://perma.cc/PU27-PY6K>]. After pleading guilty in federal district court, Russell was sentenced to five years in federal prison for possession of homemade explosives, though he was not charged as a domestic terrorist. Chokshi, *supra* note 131.

<sup>133</sup> 18 U.S.C. §§ 229, 831, 1366.

<sup>134</sup> *Id.* § 2339B; *Meet Patriot Front*, *supra* note 129. IronMarch.org, is an online forum intended to appeal to white nationalists interested in militarizing; *see Boim*, 549 F.3d at 693–94 (holding a third party liable even though he earmarked donations to Hamas specifically for educational funds because Hamas using those funds for terrorism was reasonably foreseeable). *Meet Patriot Front*, *supra* note 129; *Welcome to Hate Planet*, *supra* note 23. After this incident gained wide notoriety and the organization's existence filtered into mainstream media coverage, Atomwaffen grew in size, but many of its members also joined Vanguard America, the group with which James Fields marched in Charlottesville. *Meet Patriot Front*, *supra* note 129. Similarly, after Fields's attack, Vanguard America drew attention to itself, and, much like the fallout of the Atomwaffen arrests, many members of Vanguard America spun off to form a new organization, Patriot Front. *Id.* Patriot Front's mission statement is to transcend online discussion and carry the group's neo-Nazi ideology into real-world activism, which thus far has included disseminating flyers advertising their online presence and explicitly advocating fascism and "reconquering [one's] birthright" of the white ethnostate. *See @PatriotFront*, TWITTER, <https://twitter.com/patriotfront2?lang=eng> [<https://perma.cc/2G6W-3YZJ>]. Patriot Front is also responsible for several har-

for IronMarch.org if its hosting of Atomwaffen's content and userbase was a proximate cause of the attacks themselves.<sup>135</sup>

Although it is difficult to conceive of a plausible fact pattern in which a social media company (1) provides a platform to a homegrown extremist who (2) uses it to commit an act that (3) fits within both the definition of terrorism and the enumerated felonies that can be prosecuted as terrorism, it is not impossible.<sup>136</sup> One possible fact pattern arose in 2016, when "sovereign citizens" movement member Ammon Bundy led a group of armed militants to the Malheur National Wildlife Refuge, a federal wildlife preserve in Western Oregon, and occupied the lands for over four weeks.<sup>137</sup> Bundy and his militia made demands for the federal government to both cede its claim to the land and release prisoners who had committed arson under similar ideological justifications, and claimed they were willing to "kill and be killed" if necessary.<sup>138</sup> Before the occupation, Bundy had rallied support and coordinated his march by posting calls to arms online, including videos posted on Facebook, YouTube, and the organization's independently hosted website.<sup>139</sup> Although Bundy and his co-conspirators were not charged with

---

assessment campaigns on college campuses across the country, and its founder, eighteen-year-old Thomas Rousseau, incidentally marched next to Fields in Charlottesville. *Meet Patriot Front*, *supra* note 129. Rousseau was radicalized on IronMarch.org. *Meet Patriot Front*, *supra* note 129.

<sup>135</sup> 18 U.S.C. § 2339A; *see Boim*, 549 F.3d at 693–94 (requiring proximate cause between the provision of material support and the instant harm in order to find liability); *see, e.g., Fields v. Twitter, Inc. (Fields II)*, 217 F. Supp. 3d 1116, 1118 (N.D. Cal. 2016) (holding that ISIS's use of Twitter as an organization could not plausibly be considered a proximate cause of the shooting of five Dallas police officers, because the gunman was not himself a Twitter user), *aff'd, Fields III*, 881 F.3d 739 (9th Cir. 2018).

<sup>136</sup> *See* 18 U.S.C. §§ 2331(5), 2339A.

<sup>137</sup> Les Zaits, *Militia Takes Over Malheur National Wildlife Refuge Headquarters*, THE OREGONIAN, (Jan. 2, 2016, 9:15 PM), [http://www.oregonlive.com/pacific-northwest-news/index.ssf/2016/01/drama\\_in\\_burns\\_ends\\_with\\_quiet.html](http://www.oregonlive.com/pacific-northwest-news/index.ssf/2016/01/drama_in_burns_ends_with_quiet.html) [<https://perma.cc/5W2E-6SJK>]. The "sovereign citizens" movement is an association of right-wing antigovernment fringe groups who reject taxation, currency, and the rule of law under the theory that, when the United States was founded, the founding fathers intended a system of common law wherein individual citizens would be "sovereign," but at some point in American history this legal system was replaced by a system of admiralty law which enslaves its citizens. *Sovereign Citizens Movement*, S. POVERTY L. CTR., <https://www.splcenter.org/fighting-hate/extremist-files/ideology/sovereign-citizens-movement> [<https://perma.cc/3A68-9TY7>].

<sup>138</sup> Zaits, *supra* note 137; Press Release, U.S. Dep't of Justice, Eastern Oregon Ranchers Convicted of Arson Resentenced to Five Years in Prison (Oct. 7, 2016), <https://www.justice.gov/usao-or/pr/eastern-oregon-ranchers-convicted-arson-resentenced-five-years-prison> [<https://perma.cc/YW2K-3BXV>] (announcing the conviction of the arsonists and their sentencing under antiterrorism statutes); Siobhan Fenton, *Oregon Occupation: Militia 'Willing to Kill or Be Killed' Occupy US Wildlife Reserve*, INDEPENDENT (Jan. 3, 2016), <http://www.independent.co.uk/news/world/americas/oregon-occupation-militia-willing-to-kill-or-be-killed-occupy-us-wildlife-reserve-a6794366.html> [<https://perma.cc/WL3N-RX6X>] (reporting Ryan Bundy's statement of violent intent to journalists).

<sup>139</sup> *See, e.g., Bundy Ranch*, FACEBOOK, <https://www.facebook.com/bundy ranch/videos/937487166328092> [<https://perma.cc/T7MR-BHYN>] (archiving the Facebook page), <https://perma.cc/>

domestic terrorism, their actions—armed occupation of a federal facility for the purpose of influencing government policy, resulting in one death—could theoretically fit within the scope of crimes for which § 2339A prohibits providing material support.<sup>140</sup> Should that be the case, it is incontrovertible that the videos and other content hosted by edge providers such as Facebook were used for planning an act of domestic terror.<sup>141</sup> If hosting this content were to qualify as material support, Facebook would be criminally liable under § 2339A for providing material support in preparation for a terrorist attack.<sup>142</sup> As there is no civil remedy for domestic terrorism, Facebook could not be civilly liable under § 2339A, but plaintiffs to whom Facebook owes a duty of care could file traditional tort lawsuits under applicable theories of vicarious liability—but for the shield of § 230 of the CDA.<sup>143</sup>

### B. Section 230: The Internet's Liability Riot Shield

As terrorist activity online has grown and gained mainstream notoriety, a streak of plaintiffs have attempted to hold the social media platforms who host terrorist content civilly liable for providing material support under

---

K8GM-7Q6T (archiving the video)] (calling for sympathizers to join in the armed occupation of the wildlife refuge before it began); Bundy Ranch, FACEBOOK, <https://www.facebook.com/bundy-ranch/videos/938588846217924> [<https://perma.cc/PEL3-VT6F> (archiving the Facebook page), <https://perma.cc/S3HY-5M42> (archiving the video)] [hereinafter *Occupation Video*] (publicizing the commencement of the occupation); see also Criminal Complaint, United States v. Bundy et al., No. 3:16-cr-00051 (D.Or. Apr. 11, 2016) (detailing both the videos posted on Bundy's website "Citizens for Constitutional Freedom News Conference" as well as Bundy's extensive social media presence, both prior to and during the occupation).

<sup>140</sup> 18 U.S.C. § 2339A; see *id.* § 930(c) (prohibiting the killing of a person during an armed attack on a federal facility); *id.* § 1361 (prohibiting injuring or depredating federal government property). Both § 930(c) and § 1361 are enumerated in § 2339A. *Id.* § 2339A. One of the militants, Robert LaVoy Finicum, was killed in a shootout with the FBI during the fourth week of occupation. Pete Williams et al., *Oregon Occupation Leaders Arrested, One Dead in Shooting*, NBC NEWS (Jan. 26, 2016, 8:48 AM), <https://www.nbcnews.com/news/us-news/oregon-occupation-leader-ammon-bundy-arrested-law-enforcement-sources-n504911> [<https://perma.cc/M828-A7Y6>]. The felony murder rule could impart liability on Finicum's co-conspirators, who were attempting to escape the police. *Id.*; see 18 U.S.C. § 1111 (imputing culpability for any killing that occurs during the commission of a dangerous felony to anyone guilty of the felony, even when the felon is not the killer).

<sup>141</sup> See 18 U.S.C. § 930(c) (prohibiting the killing of a person during an armed attack on a federal facility); *id.* § 1361 (prohibiting injuring or depredating federal government property); *supra* note 139–140 and accompanying text.

<sup>142</sup> See 18 U.S.C. § 2339A; *Boim*, 549 F.3d at 693–94 (holding a third party liable for providing material support for providing funds to a terrorist group, even though he did not know those funds would be used to support terrorism); *supra* note 139–140 and accompanying text.

<sup>143</sup> See 18 U.S.C. § 2339A; Telecommunications Act of 1996 § 230, 47 U.S.C. § 230(c)(1) (2012).

§ 2339A and § 2339B.<sup>144</sup> Because civil remedy only exists for international terrorism, only victims of international terrorism have attempted suit under these statutes, and all have failed.<sup>145</sup>

The most prominent of attempts to undermine § 230 is *Fields v. Twitter, Inc.*, wherein the family members of two government contractors shot and killed in Jordan by an ISIS gunman brought suit against Twitter for allowing ISIS to make use of its services.<sup>146</sup> The case was dismissed twice, with the court finding each claim barred by the CDA.<sup>147</sup> The plaintiffs argued that in allowing ISIS to sign up for accounts, Twitter had provided material support to a DFTO in violation of § 2339B.<sup>148</sup> Anticipating the CDA challenge, the plaintiffs argued that while the CDA prevents civil plaintiffs from holding an edge provider liable for engaging in “publishing activities,” a publishing activity requires making content-based editorial decisions, and Twitter’s decision to provide accounts to ISIS was content neutral, and thus not a “publishing activity” as defined and protected by the CDA.<sup>149</sup> The court was not convinced, holding that any decision to provide or refuse an account to a user based on affiliation with ISIS is a content-based decision qualifying as a publishing activity.<sup>150</sup> As a result, Twitter could not be held liable for providing accounts to members of ISIS.<sup>151</sup> The *Fields* court was strict in its application of the CDA, writing that any pleading that mentions Twitter’s decision to exclude something from its platform is inherently an attempt to treat Twitter as a publisher because it describes

---

<sup>144</sup> See, e.g., *Gonzalez*, 282 F. Supp. 3d at 1154–55; *Pennie*, 281 F. Supp. 3d at 877; *Cohen*, 252 F. Supp. 3d at 146; see also *infra* notes 146–196 and accompanying text (discussing several of these recent cases).

<sup>145</sup> *Goldman*, *Seventh Lawsuit*, *supra* note 92; see *infra* notes 146–196 and accompanying text (explaining the respective courts’ rationales for dismissing the suits).

<sup>146</sup> *Fields II*, 217 F. Supp. 3d at 1117; *Fields v. Twitter, Inc. (Fields I)*, 200 F. Supp. 3d 964, 966 (N.D. Cal. 2016). Plaintiffs specifically alleged that ISIS uses Twitter as a recruiting, fundraising, and communications platform, and had recruited over 30,000 members through Twitter within one year. *Fields I*, 200 F. Supp. 3d at 967–68.

<sup>147</sup> *Fields II*, 217 F. Supp. 3d at 1119; *Fields I*, 200 F. Supp. at 966.

<sup>148</sup> *Fields II*, 217 F. Supp. 3d at 1119.

<sup>149</sup> *Id.* at 1122. More specifically, plaintiffs argued that their complaint was content-neutral, because ISIS’s actual activities on the platform were irrelevant—the simple act of furnishing accounts to ISIS members was itself a provision of material support to a DFTO. *Id.* Twitter countered, and the court agreed, that both the first and second complaints relied on descriptions of ISIS-related content. *Id.* The court further held that, even had the complaint been content-neutral, the decision to furnish an account is functionally no different than the essential editorial decision of a publisher to print or not print content, and the complaint was therefore still dependent on Twitter’s conduct as a publisher. *Id.* at 1124–25.

<sup>150</sup> *Id.* at 1124–25. The plaintiffs’ claims also failed because they did not sufficiently allege proximate cause, a requirement for civil suits. *Id.* at 1126–27. The court held that ISIS’s use of Twitter as an organization could not plausibly be considered a proximate cause of the shooting, because the gunman was not himself a Twitter user. *Id.*

<sup>151</sup> *Id.* at 1124–25.

the content Twitter chooses to host.<sup>152</sup> Decisions over what content to host are content-based publication decisions, and Twitter's provision of accounts to its users was in fact a decision over what content it hosts.<sup>153</sup> The suit was therefore barred by the CDA.<sup>154</sup>

*Fields* is one of many lawsuits that have failed for the same reason.<sup>155</sup> A litany of dismissals has permeated district courts in recent years, with all failing to allege liability without treating the edge provider as a publisher.<sup>156</sup> Some suits have attempted to challenge the statute itself: in *Gonzalez v. Google, Inc.*, in addition to claiming that Google's hosting of content was not a publishing activity, the plaintiff also unsuccessfully alleged that when Congress passed the Justice Against Sponsors of Terrorism Act ("JASTA") in 2016, amending 18 U.S.C. § 2333 to create civil liability, it effectively repealed § 230.<sup>157</sup> Once again, the court was unconvinced, holding that § 230 was always intended to limit civil liability and, absent express language, should not be interpreted otherwise.<sup>158</sup> Every adjudicated suit that has attempted this argument has failed.<sup>159</sup>

The most recent (and unsuccessful) innovation in legal theories attempting to sidestep the CDA began after the 2016 Pulse nightclub shooting.<sup>160</sup> In 2016, an ISIS-affiliated gunman opened fire on an Orlando gay nightclub, Pulse, killing forty-nine and wounding fifty-eight.<sup>161</sup> When families of shooting victims brought suit against Twitter, Facebook, and Google, they anticipated the CDA bar and claimed to have founded their theory of

---

<sup>152</sup> *Id.*

<sup>153</sup> *Id.*

<sup>154</sup> *Id.* at 1125. On appeal, the Federal Court of Appeals for the Ninth Circuit sidestepped the issue, instead focusing on the plaintiffs' failure to adequately allege proximate cause. *See Fields III*, 881 F.3d 739, 749–50 (9th Cir. 2018).

<sup>155</sup> *See, e.g., Gonzalez*, 282 F. Supp. 3d at 1150 (dismissing plaintiff's claim as barred by the CDA); *Cohen*, 252 F. Supp. 3d at 159–60 (dismissing both plaintiffs' claims as barred by the CDA).

<sup>156</sup> *See, e.g., Gonzalez*, 282 F. Supp. 3d at 1150 (dismissing the plaintiff's claim as barred by the CDA); *Cohen*, 252 F. Supp. 3d at 159–60 (dismissing both plaintiffs' claims as barred by the CDA). Notably, several of these suits were filed by the same group: 1-800-LAW-FIRM. *Anti-Terrorism, Terror Victims v. Social Media Giants*, 1-800-LAW-FIRM, <https://www.1800lawfirm.com/practice-areas/anti-terrorism> [<https://perma.cc/TS8X-3XRJ>].

<sup>157</sup> *Gonzalez*, 282 F. Supp. 3d at 1159; *see* Justice Against Sponsors of Terrorism Act, Pub. L. No. 114-222, 130 Stat. 852 (2016); 47 U.S.C. § 230.

<sup>158</sup> *Gonzalez*, 282 F. Supp. 3d at 1159–60.

<sup>159</sup> Goldman, *Seventh Lawsuit*, *supra* note 92; *see, e.g., Pennie*, 281 F. Supp. 3d at 889; *Cohen*, 252 F. Supp. 3d at 159–60.

<sup>160</sup> *See Crosby v. Twitter, Inc.*, No. 2:16-cv-14406, 2017 WL 4224194 at \*3. (E.D. Mich. Mar. 31, 2017).

<sup>161</sup> Lizette Alvarez & Richard Pérez Peña, *Orlando Gunman Attacks Gay Nightclub, Leaving 50 Dead*, N.Y. TIMES (June 12, 2016), <https://www.nytimes.com/2016/06/13/us/orlando-nightclub-shooting.html> [<https://perma.cc/MSX3-ECD2>].

liability not on providing accounts, but on shared advertising agreements.<sup>162</sup> The plaintiffs of *Crosby v. Twitter, Inc.*, first argued that Twitter, Facebook, and Google’s “provision of the infrastructure” of their platforms was material support because it allowed ISIS to flourish online.<sup>163</sup> To circumvent the CDA, however, the plaintiffs grounded their argument in targeted advertising agreements.<sup>164</sup> Social media sites engineer algorithms to target advertisements to specific demographics of consumers, including ideological demographics, and site personnel must manually approve any advertiser requesting use of some of those algorithms.<sup>165</sup> Plaintiffs argued that because Twitter, Facebook, and Google exercise control over advertising, when they combined ISIS postings with their own advertisements, the result was a creation of content.<sup>166</sup> In creating content, plaintiffs argued, these edge providers were not computer services, but rather content providers, and therefore not entitled to immunity under the CDA.<sup>167</sup> Like *Fields*, *Crosby* was ultimately dismissed for lack of proximate causation between ISIS’s Twitter accounts and the shooter himself.<sup>168</sup> The second question of whether § 230 applies when combining advertisements with posts remains unresolved.<sup>169</sup>

Despite the seeming invulnerability § 230 provides to edge providers, § 230 is in danger.<sup>170</sup> In *Gonzalez*, the plaintiff unsuccessfully argued that Congress’ passage of JASTA implicitly repealed § 230.<sup>171</sup> The court’s disa-

<sup>162</sup> See First Amended Complaint, *Crosby*, 2017 WL 4224194, at \*3.

<sup>163</sup> *Id.*

<sup>164</sup> *Id.*

<sup>165</sup> See *id.*; Alex Andrada-Walz, *What Can and Can’t You Do with Political Advertising on Facebook?*, SPATIALLY (Feb. 26, 2018) <http://www.spatially.com/blog/political-advertising-on-facebook> [<https://perma.cc/FR5B-4F7F>] (explaining that Facebook’s text analysis of its users separates them into distinct political affiliation groups, and political advertisers may target these groups once they provide documentation to Facebook staff verifying identity and location); Facebook Advertising Targeting, FACEBOOK, <https://www.facebook.com/business/ads/ad-targeting> [<https://perma.cc/RTT9-QD5X?type=image>] (enabling advertisers to target algorithmically selected groups of users).

<sup>166</sup> First Amended Complaint, *supra* note 162, at \*3.

<sup>167</sup> *Id.* When an edge provider creates content, they are an “information content provider” for CDA purposes, and the CDA does not exempt content providers from liability. 47 U.S.C. § 230(c).

<sup>168</sup> *Fields*, 881 F.3d at 749–50; *Crosby*, 303 F. Supp. 3d at 570.

<sup>169</sup> *Crosby*, 303 F. Supp. 3d at 570. The presiding judge declined to address the CDA because without adequately pleaded causation, the plaintiffs had not stated any claim for which a court could grant relief. *Id.*

<sup>170</sup> See Eric Goldman, *Senate’s “Stop Enabling Sex Traffickers Act of 2017”—and Section 230’s Imminent Evisceration*, TECH. & MARKETING L. BLOG (July 31, 2017), <https://blog.ericgoldman.org/archives/2017/07/senates-stop-enabling-sex-traffickers-act-of-2017-and-section-230s-imminent-evisceration.htm> [<https://perma.cc/6SKQ-EDFT>]; *infra* notes 171–196 and accompanying text.

<sup>171</sup> *Gonzalez*, 282 F. Supp. 3d at 1159. See generally Justice Against Sponsors of Terrorism Act (JASTA), Pub. L. 114-222, 130 Stat. 852 (2016). JASTA was enacted to “hold foreign sponsors of terrorism that target the United States accountable in Federal courts” by eliminating im-

greement was founded in JASTA's irrelevance to the CDA; JASTA does not reference the CDA or computer service providers, nor did Congress make such reference during the bill's passage.<sup>172</sup> The CDA remains intact so long as direct congressional action does not erode it—which it might.<sup>173</sup>

On April 11, 2018, President Donald Trump signed the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (“FOSTA”) into law.<sup>174</sup> FOSTA expressly amends § 230 to revoke liability protection for any Internet service or edge provider in cases involving sex trafficking by force or child sex trafficking.<sup>175</sup> Sponsored by Rep. Ann Wagner (R-MO) and drafted in response to Backpage.com's facilitation of sex trafficking, the law first finds that § 230 was “never intended to provide legal protection to websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims.”<sup>176</sup> Next, it broadly amends § 230 to permit civil suit against an Internet computer service that violates specific federal child sex trafficking laws, federal laws which prohibit sex trafficking by force, or equivalent state laws.<sup>177</sup> 18 U.S.C. § 1595 allows the victim of a sex trafficking crime to bring suit against both the perpetrator and anyone who benefits from the sex trafficking, and FOSTA also amends § 230 to expressly allow suits brought under § 1595.<sup>178</sup> Section 1595 is the sex trafficking equivalent of § 2333, and it functions similarly in that it creates civil liability not only for perpetrators, but also for anyone who knowingly benefits from participating in anything they knew (or should have known) violated sex trafficking law.<sup>179</sup> Finally, the law expressly states that should an edge provider recklessly disregard that their platform has been used to pro-

---

munity for foreign states who either directly or by omission sponsor terrorism in the United States. *Gonzalez*, 282 F. Supp. 3d at 1160. The Senators sponsoring JASTA stated they intended the law to “close a loophole” that prevented families of 9/11 first responders from “pursu[ing] their claims for justice against those who sponsored those acts of terrorism on U.S. homeland.” *Id.*

<sup>172</sup> *Gonzalez*, 282 F. Supp. 3d at 1159–60.

<sup>173</sup> See, e.g., Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (2018) (creating an exception in the CDA permitting suit against edge providers in sex trafficking cases); see also *infra* notes 174–196 and accompanying text.

<sup>174</sup> Allow States and Victims to Fight Online Sex Trafficking Act of 2017 § 2.

<sup>175</sup> *Id.*

<sup>176</sup> *Id.* Backpage.com was an online classified advertising website, similar to Craigslist. Press Release, Dep't of Justice, Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment (Apr. 9, 2018). Adult sex workers used its “adult services” sections to advertise their services, but the site also included advertisements for child prostitution. *Id.* In 2018, the Department of Justice seized Backpage.com and charged its founders with 93 counts relating to a conspiracy to facilitate prostitution. *Id.*

<sup>177</sup> Allow States and Victims to Fight Online Sex Trafficking Act § 4.

<sup>178</sup> *Id.*

<sup>179</sup> *Id.*; see 18 U.S.C. § 2333 (creating liability for violations of § 2339A and § 2339B, which prohibit providing material support in violation of terrorism law).

mote or facilitate sex trafficking, civil litigants may file suit against them.<sup>180</sup> In passing FOSTA, Congress declined to adopt the Senate version of the bill, introduced by Senator Rob Portman (R-OH) as the Stop Enabling Sex Traffickers Act of 2017 (“SESTA”).<sup>181</sup> SESTA did not include the “reckless disregard” language, and critics of both SESTA and FOSTA regarded SESTA as considerably less corrosive to the CDA.<sup>182</sup>

Sex trafficking is not the only proposed exception to the CDA: in 2014, Representative Jackie Speier (D-CA) worked to draft legislation that would criminalize “revenge porn”—non-consensual distribution of intimate content—which she claimed would strip edge providers of the ability to raise § 230 immunity.<sup>183</sup> She subsequently introduced the Intimate Privacy Protection Act (“IPPA”) in 2016, but the bill was amended to specifically exempt interactive computer service providers, including ISPs and edge providers, likely at the behest of Google.<sup>184</sup> Similar to FOSTA, IPPA would prohibit an edge provider from recklessly disregarding whether the sexually explicit content being distributed on its platform is nonconsensual.<sup>185</sup>

Both FOSTA and IPPA represent attempts to curtail the CDA, and both prohibit reckless disregard for support of sex traffickers or revenge porn.<sup>186</sup> Consequently, both permit convicting edge providers of recklessly providing support for each respective crime.<sup>187</sup> As commenters have already pointed out, a determined Congress, using the public safety justification at the hearts of these bills, could easily transpose the frameworks of FOSTA or

<sup>180</sup> Allow States and Victims to Fight Online Sex Trafficking Act § 3; 18 U.S.C. § 2421A.

<sup>181</sup> Allow States and Victims to Fight Online Sex Trafficking Act § 3; Stop Enabling Sex Traffickers Act of 2017, S.1693, 115th Cong. (2017).

<sup>182</sup> *Id.*; see Goldman, *supra* note 170 (highlighting that, unlike FOSTA, SESTA would not have opened up CDA exceptions to include state claims).

<sup>183</sup> Steven Nelson, *Federal ‘Revenge Porn’ Bill Will Seek to Shriveled Booming Internet Fad*, U.S. NEWS & WORLD REP. (Mar. 26, 2014, 6:01 PM), <https://www.usnews.com/news/articles/2014/03/26/federal-revenge-porn-bill-will-seek-to-shriveled-booming-internet-fad> [<https://perma.cc/5GSP-MU8H>].

<sup>184</sup> Intimate Privacy Protection Act of 2016, H.R. 5896, 114th Cong. (2016); see Sarah Jeong, *New Revenge Porn Bill Shows Silicon Valley’s Influence in Politics*, MOTHERBOARD (July 15, 2016, 4:28 PM), [https://motherboard.vice.com/en\\_us/article/53d59z/new-revenge-porn-bill-shows-silicon-valleys-influence-in-politics](https://motherboard.vice.com/en_us/article/53d59z/new-revenge-porn-bill-shows-silicon-valleys-influence-in-politics) [<https://perma.cc/RU8Y-3BNJ>]. Google opposed the initial draft of the bill but does not oppose the current version. See Jeong, *supra*.

<sup>185</sup> See Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong. (2017) (“[W]hoever . . . owns, manages, or operates . . . an interactive computer services and . . . acts in reckless disregard of the fact that such conduct contributed to sex trafficking . . .”); Intimate Privacy Protection Act of 2016, H.R. 5896, 114th Cong. (2016).

<sup>186</sup> See Allow States and Victims to Fight Online Sex Trafficking Act § 3; Intimate Privacy Protection Act of 2016, H.R. 5896, 114th Cong. (2016).

<sup>187</sup> See Allow States and Victims to Fight Online Sex Trafficking Act § 3 (applying liability to intermediaries who facilitate sex trafficking); Intimate Privacy Protection Act of 2016, H.R. 5896, 114th Cong. (2016) (applying liability to intermediaries who host “revenge porn”).

IPPA onto terrorism material support law.<sup>188</sup> IPPA, FOSTA, and § 2339A share similar skeletons, in that they all prohibit a party from recklessly disregarding whether their support benefits a crime.<sup>189</sup>

While § 2333 suits against edge providers may fall to the CDA, elsewhere, the CDA is being weakened in court.<sup>190</sup> In 2016, the Ninth Circuit held in *Doe No. 14 v. Internet Brands, Inc.* that when the plaintiff attempted to hold an edge provider liable for the actions of its users, she was not barred by the CDA.<sup>191</sup> The plaintiff alleged that Internet Brands was aware that two of its male users were using the platform to organize attacks on female users.<sup>192</sup> The court held that the plaintiff was not attempting to hold Internet Brands liable as the publisher of the men's speech, but rather that Internet Brands had negligently failed to warn her of the danger.<sup>193</sup> The failure to warn was not a publishing decision, as she was not asking Internet Brands to add or remove content, and therefore the suit was not barred by the CDA because an edge provider's duty to warn did not implicate its ability to publish content, and the suit was therefore not barred by the CDA.<sup>194</sup> Another dent in the shield appeared in *Huon v. Denton*, where in 2016 the Federal Court of Appeals for the Seventh Circuit did not permit CDA immunity for the website Gawker in a defamation suit because Gawker was a content provider.<sup>195</sup> Gawker had assisted in developing the defamatory speech by inviting users to post inflammatory and often defamatory comments, some of them authored by anonymous Gawker employees.<sup>196</sup>

---

<sup>188</sup> 18 U.S.C. § 2339A; *see, e.g.*, Goldman, *supra* note 170 (pointing out direct parallels between challenges to § 230 stemming from terrorism and sex trafficking).

<sup>189</sup> 18 U.S.C. § 2339A; Allow States and Victims to Fight Online Sex Trafficking Act § 3; Intimate Privacy Protection Act.

<sup>190</sup> *See, e.g.*, *Doe No. 14 v. Internet Brands, Inc.*, 824 F.3d 846, 850 (9th Cir. 2016); *see also infra* notes 194–196 and accompanying text.

<sup>191</sup> *Internet Brands*, 824 F.3d at 851.

<sup>192</sup> *Id.* Internet Brands provided a service wherein aspiring models could post information for professional networking purposes. *Id.* at 848. Jane Doe alleged that two individuals used the website to fraudulently pose as talent agents and lure victims to a fake audition, where they were then drugged, raped, and recorded for digital distribution. *Id.* Doe alleged that she was a victim of this scheme in 2011, and that Internet Brands had been aware of the perpetrators' activities as early as 2010. *Id.* at 848–49.

<sup>193</sup> *Id.* at 850–51.

<sup>194</sup> *Id.*

<sup>195</sup> *Huon v. Denton*, 841 F.3d 733, 741–42 (7th Cir. 2016). The plaintiff in *Huon* sued now-defunct news entertainment company Gawker and its founder, Nick Denton, for defamation after its employees curated user comments and posted their own anonymous comments to an allegedly defamatory news article, for the purposes of generating traffic. *Id.*

<sup>196</sup> *Id.*

### III. IF THE LAW SHOULD CHANGE, HOW?: PROPOSING MODEST AMENDMENTS TO DOMESTIC TERRORISM LAW

“Maybe someone dies in a terrorist attack coordinated on our tools.”<sup>197</sup> BuzzFeed reporters uncovered these words in an internal memo penned in 2016 by Facebook Vice President Andrew Bosworth.<sup>198</sup> In the memo, Bosworth justifies the risks of collateral damage that Facebook poses as an acceptable cost of Facebook’s mission of connecting people across the world.<sup>199</sup> Current law seems to agree—but should it?<sup>200</sup>

Liability, or at least vulnerability to suit, is already not as far-fetched as edge providers would like.<sup>201</sup> It is not impossible to prosecute an edge provider for violating 18 U.S.C. § 2339A, should the government be so inclined.<sup>202</sup> Section 2339A may not permit civil suit, but victims of domestic terrorism can still pursue justice through traditional tort remedies.<sup>203</sup> The only true legal barrier for plaintiffs looking to hold a tech company liable for providing domestic terrorists with a platform is § 230 of the CDA, and it is in danger.<sup>204</sup> With escalating domestic terrorism and consequent pressure on tech companies to responsibly monitor their platforms, it is worth contemplating if and how the framework for material support liability in do-

<sup>197</sup> Ryan Mac et al., *Growth at Any Cost: Top Facebook Executive Defended Data Collection in 2016 Memo—And Warned That Facebook Could Get People Killed*, BUZZFEED NEWS (Mar 29, 2018) <https://www.buzzfeednews.com/article/ryanmac/growth-at-any-cost-top-facebook-executive-defended-data> [<https://perma.cc/L5RH-457E>].

<sup>198</sup> *Id.* Bosworth wrote the memo one day after a deadly Chicago shooting was recorded and streamed on Facebook Live, the company’s video streaming service. *Id.* A Facebook employee, disgruntled with the lack of response from either Mark Zuckerberg or the company, produced the memo to journalists at BuzzFeed after Bosworth was tapped for a promotion. *Id.* Zuckerberg and Bosworth have both since denounced the views expressed in the memo, which is known internally as “The Ugly” and is still available for Facebook employees to view. *Id.*

<sup>199</sup> *Id.*  
<sup>200</sup> *See id.*; *Zeran v. America Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997) (finding that Congress’s intent in passing the § 230 was to eliminate the “specter of tort liability”); *infra* notes 202–251 and accompanying text (weighing the speech and economic interests of maintaining the § 230 against the threat of rapid online radicalization).

<sup>201</sup> *See* Goldman, *supra* note 170 (arguing that FOSTA’s passage could be the first of many new exceptions to the CDA); *infra* notes 202–204 and accompanying text.

<sup>202</sup> *See* 18 U.S.C. § 2339A (2012) (criminalizing providing material support for an act of terrorism, not excluding domestic terrorism). By damaging a federal facility and participating in a shootout that resulted in the death of a person, the Bundy occupation ostensibly violated federal terrorism law. *See id.* § 1361 (prohibiting injuring or depredating federal government property); *id.* § 930(c) (prohibiting the killing of a person during an armed attack on a federal facility); Criminal Complaint, *USA v. Bundy et al.*, 3:16-cr-00051 (D.Or. 2016) (detailing extensive social media presence of Bundy both prior to and during the occupation); *Occupation Video*, *supra* note 139.

<sup>203</sup> 18 U.S.C. § 2339A.

<sup>204</sup> *See e.g.*, Allow States and Victims to Fight Online Sex Trafficking Act of 2017, H.R. 1865, 115th Cong. (2017); 18 U.S.C. § 2421A (2018) (substantially amending § 230 to exclude sex trafficking crimes and civil actions from its protections, including when an Internet computer service recklessly disregards whether its users engage in sex trafficking); 18 U.S.C. § 2339A.

mestic terrorism law should be revised.<sup>205</sup> This Part posits a few possibilities for the future of domestic terror law and analyzes potential outcomes, should those possibilities come to pass.<sup>206</sup> Section A discusses the infeasibility and inadvisability of repealing § 230.<sup>207</sup> Section B suggests providing a civil remedy for domestic terror victims via § 2339A and outlines how such a remedy's benefits would outweigh any consequences.<sup>208</sup>

*A. If It Ain't Broke: The Inadvisability of Repealing or  
Further Altering 18 U.S.C. § 230(c)*

The United States is no stranger to curtailing individual civil liberties in the interest of more effectively fighting foreign terror threats.<sup>209</sup> The CDA is already facing imminent erosion on other fronts, suggesting that further congressional action against § 230 in the terror sphere is possible.<sup>210</sup> A full repeal of § 230 would, of course, be catastrophic to the Internet.<sup>211</sup> While the free speech implications of holding massive platforms liable for their userbases are debatable, the logistical implications are not.<sup>212</sup>

<sup>205</sup> See 18 U.S.C. § 2339A; *Hate Map*, *supra* note 12 (documenting an increase in the number of active hate groups from 457 in 1999 to 917 in 2016); *see, e.g.*, Levin, *supra* note 28 (suggesting that YouTube algorithms that redirect viewers of political content to increasingly extreme content, some of it terroristic in nature, are responsible for radicalization, and criticizing YouTube for not adequately addressing the problem).

<sup>206</sup> See *infra* notes 209–251 and accompanying text.

<sup>207</sup> See *infra* notes 209–222 and accompanying text.

<sup>208</sup> See *infra* notes 223–251 and accompanying text.

<sup>209</sup> See *e.g.*, Military Commissions Act of 2006, Pub. L. No. 109-366 § 5, 120 Stat. 2600 (2006) (suspending *habeas corpus* rights for any person deemed an “unlawful enemy combatant engaged in hostilities . . . against the United States”—a suspension which was later held unconstitutional in *Boumediene v. Bush*, 553 U.S. 723 (2008)); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56 § 215, 115 Stat. 272 (2001) (permitting the federal government to obtain secret orders requiring telecommunications companies to produce any “tangible things” relevant to fighting international terrorism, including detailed customer records).

<sup>210</sup> See *e.g.*, Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (amending the CDA to add an exception for liability against edge providers); *supra* notes 171–196 and accompanying text.

<sup>211</sup> See *Cohen v. Facebook, Inc.*, 252 F. Supp. 3d 140, 155 (E.D.N.Y. 2017) (noting that § 230 was enacted to “maintain the robust nature of Internet communication,” and accordingly, Congress avoided creating law that would chill speech where speakers might fear tort liability); *infra* notes 212–222 and accompanying text.

<sup>212</sup> Compare Eric Goldman, *Congress Is About to Ruin Its Online Free Speech Masterpiece*, TECH. & MARKETING L. BLOG (Sept. 24, 2017) <https://blog.ericgoldman.org/archives/2017/09/congress-is-about-to-ruin-its-online-free-speech-masterpiece-cross-post.htm> [<https://perma.cc/MM5V-AWKD>] (framing § 230 as one of—if not *the*—most important pieces of free speech legislation ever passed and arguing that § 230 is vital to the continued existence of the Internet), with DANIELLE CITRON, HATE CRIMES IN CYBERSPACE, 191–92 (2014) (asserting that the Internet, like any forum for discussion such as a workplace, home, or coffee shop, does not merit special speech protections or exemptions from tort, criminal, or civil rights laws).

The CDA has provided protection for Internet edge providers since the early days of the Internet, well before the modern social media ecosystem was established.<sup>213</sup> This protection has enabled technologies and tech empires to develop unfettered by any need to incorporate monitoring systems to ameliorate their own liability.<sup>214</sup> To create liability now would also create a logistical nightmare for edge providers as large as Facebook or Twitter.<sup>215</sup> It is unreasonable to expect edge providers, particularly tech social media giants with incomprehensibly large userbases, to actively monitor massive quantities of data simply to protect themselves from suit.<sup>216</sup> Even if liability were limited to edge providers who had actual—not just constructive—notice of unlawful behavior within their control to suspend, yet chose not to

---

<sup>213</sup> Telecommunications Act of 1996, Pub. L. No. 104-104 § 509, 110 Stat. 56 (1996), 47 U.S.C. § 230(c) (2012). Section 230 was passed in 1996. *Id.* Although forum technologies like bulletin board systems (computer servers connecting to terminals) functioned as discussion boards in the 1980s, these early forums were hosted on private servers with comparatively small userbases. See Saqib Shah, *The History of Social Networking*, DIGITAL TRENDS (May 14, 2016) <https://www.digitaltrends.com/features/the-history-of-social-networking> [<https://perma.cc/CF5E-FTNS>]. Social media began its corporatization in earnest in 1993, when America Online (“AOL”) added Usenet, a worldwide distributed discussion system, to its available features. See Jason Koebler, *It’s September, Forever*, MOTHERBOARD, (Sept. 30, 2015) [https://motherboard.vice.com/en\\_us/article/nze8nb/its-september-forever](https://motherboard.vice.com/en_us/article/nze8nb/its-september-forever) [<https://perma.cc/9CRV-X9UZ>]. Social media as we know it today did not fully take shape until the advent of Friendster in 2002 and LinkedIn in 2003, both of which implemented “connection” systems like those still in use by most modern social media platforms. See Shah, *supra*. LinkedIn ultimately became the first major modern social network to have an initial public offering, going public in 2011. Nicole Perloth, *And the First IPO Goes to... LinkedIn*, FORBES (Jan. 27, 2011) <https://www.forbes.com/sites/nicoleperloth/2011/01/27/and-the-first-ipo-is-linkedin> [<https://perma.cc/VHJ9-GNDE>].

<sup>214</sup> *The Latest Developments in Combating Online Sex Trafficking: Hearing Before the Subcomm. on Commc’ns and Tech. of the Comm. on Energy and Commerce*, 115th Cong. 48–49 (2017) (statement of Eric Goldman, Professor, Santa Clara University School of Law) [hereinafter Committee Hearing].

<sup>215</sup> *Id.*; see, e.g., *The Top 20 Valuable Facebook Statistics—Updated March 2019*, ZEPHORIA DIGITAL MARKETING, <https://zephoria.com/top-15-valuable-facebook-statistics> [<https://perma.cc/7P7N-E4RU>]. As of the end of 2018, Facebook had 2.32 billion monthly active users. *Id.* Likewise, YouTube receives over sixty-three million daily users, and users upload three hundred hours of video every minute. *YouTube Revenue and Usage Statistics (2018)*, BUSINESS OF APPS, <http://www.businessofapps.com/data/youtube-statistics> [<https://perma.cc/EFD3-Q9GX>]. On Twitter, users produce over six thousand tweets per second, and over five hundred million tweets per day. INTERNET LIVE STATS, <http://www.internetlivestats.com/twitter-statistics> [<https://perma.cc/XN8M-CT3P>].

<sup>216</sup> See Goldman, *supra* note 170 (arguing that without the CDA, online social media companies would be existentially threatened by the financial exposure to litigation). Goldman also argues that even strict knowledge requirements would create a “moderator’s dilemma,” where an edge provider would either need to monitor all content and accept liability where it failed, or completely abandon any attempt at moderation. Eric Goldman, *New House Bill (Substitute FOSTA) Has More Promising Approach to Regulating Online Sex Trafficking*, TECHN. & MARKETING L. BLOG (Dec. 11, 2017) <https://blog.ericgoldman.org/archives/2017/12/new-house-bill-substitute-fosta-has-more-promising-approach-to-regulating-online-sex-trafficking.htm> [<https://perma.cc/MN7Y-5G7U>].

curtail it, the sheer breadth of potential causes of action against a publisher of content would require extraordinary investment in both algorithmic monitoring systems and monitoring staff.<sup>217</sup> Many large tech companies are already unprofitable, and requiring an investment of this magnitude could strain their capital to a breaking point.<sup>218</sup> Moreover, imposing an actual knowledge requirement may incentivize tech companies to actively avoid gaining any dangerous knowledge by abandoning content moderation altogether.<sup>219</sup>

One alternative to full repeal is a narrow exclusion for suits pursued under 18 U.S.C. § 2333, much like the exclusion in FOSTA, but while this solution is less inherently unfair than a full repeal, not only would it cause the same logistical problems for edge providers, it would also provide no remedy for victims of domestic terror.<sup>220</sup> With a full repeal, victims of domestic terror could at least file traditional tort suits, but a narrow § 2333 exception would preclude even that.<sup>221</sup> Without addressing remedies for domestic terror victims, any repeal or narrowing of the CDA creates far more problems than it solves.<sup>222</sup>

### *B. A Good Compromise Leaves Both Sides Equally Dissatisfied*

To properly balance the interests of tech companies and victims of domestic terrorism, Congress should amend § 2333 to expand § 2339A civil causes of action to include providing material support to domestic terrorist acts.<sup>223</sup> Such an amendment would be narrow enough in its applicability to

<sup>217</sup> See Eric Goldman, *Sex Trafficking Exceptions to Section 230*, SANTA CLARA UNIV. LEGAL STUDIES RESEARCH PAPER NO. 13-71, 1 (2017) (testifying to Congress about the logistical difficulties of requiring every computer service to monitor their platforms for any content that would give rise to litigation).

<sup>218</sup> Committee Hearing, *supra* note 214; Angelo Young, *Why Are There So Many Billionaires Leading Money-Losing Companies?*, SALON (June 6, 2017) <https://www.salon.com/2017/06/06/why-are-there-so-many-billionaires-leading-money-losing-companies> [<https://perma.cc/M67V-4P8A>]. In 2012, almost one-third of Twitter's total expenditures went to operational costs, including facilities, training, and staff compensation. David Ingold, *Where Twitter Spends and Makes Its Money*, BLOOMBERG (Nov. 7, 2013) <https://www.bloomberg.com/graphics/infographics/twitter-readies-ipo-struggles-to-turn-a-profit.html> [<https://perma.cc/MNA4-ATVZ>].

<sup>219</sup> Committee Hearing, *supra* note 214. This phenomenon is known as the “moderator’s dilemma.” *Id.* Because § 230 does not have a knowledge requirement, tech companies are free to moderate their platforms without concern that stumbling upon bad user content will create liability. *Id.*

<sup>220</sup> See 18 U.S.C. § 2333 (permitting civil suit for victims of foreign terrorism using § 2339A and § 2339B, but omitting domestic terror acts).

<sup>221</sup> See *id.*

<sup>222</sup> See Committee Hearing, *supra* note 214; (testifying to the logistical difficulties of moderating websites with massive userbases in the absence of CDA protection); *supra* notes 209–222 and accompanying text.

<sup>223</sup> See 18 U.S.C. §§ 2333, 2339A; *infra* notes 226–251 and accompanying text.

avoid ravaging the modern Internet landscape while addressing an enforcement gap and encouraging better practices by edge providers.<sup>224</sup>

Any discussion of holding edge providers liable for the speech of their users inevitably invites debate over whether such a policy implicates free speech concerns.<sup>225</sup> An argument against stronger domestic terrorism law in general is that a framework in parity with foreign terror law could easily result in classifying political activists as terrorists, thereby chilling speech.<sup>226</sup> While this more generalized concern should not be downplayed, domestic terror is prosecuted based on defendants' actions, not their affiliation, and the limited toolset in § 2339A itself means that the reach of any chilling effect is just as limited.<sup>227</sup> Section 2339A criminalizes knowingly providing material support for domestic terror attacks, but the scope of what constitutes a domestic terror attack is narrow.<sup>228</sup> Any attack at issue must fall within several enumerated offenses and must fit the definition of domestic terrorism as provided by § 2331(5).<sup>229</sup> To be guilty, a third party must then provide material resources or support while knowing that it will be used in preparation for an attack.<sup>230</sup> Moreover, for liability to apply to a third party, those attacks must fall under one of few enumerated, specific offenses; simple harm to human life will not do.<sup>231</sup> The recent spate of lawsuits against Twitter, YouTube, and Google, while arguably frivolous given the strength of the CDA were still only possible because the perpetrators of the attacks were associated with DFTOs and thus fell within the far broader

---

<sup>224</sup> See 18 U.S.C. § 2333; *infra* notes 226–251 and accompanying text.

<sup>225</sup> Compare Goldman, *supra* note 212 (arguing that curtailing the CDA chills free speech by causing moderators dilemmas), with Citron, *supra* note 212 (arguing against the assumption that the Internet is a forum that merits special speech protections).

<sup>226</sup> See Reilly, *supra* note 50 (discussing law enforcement's reluctance to use the term "terrorism" in the domestic sphere for fear of inappropriately labeling political opposition).

<sup>227</sup> Compare 18 U.S.C. § 2339A (penalizing providing material support to terrorist actions), with 18 U.S.C. § 2339B (penalizing providing material support to designated foreign terrorist organizations).

<sup>228</sup> *Id.* § 2339A.

<sup>229</sup> *Id.*

<sup>230</sup> *Id.*; see *id.* § 2331(5)(B) (requiring that an attack be intended "to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping" in order to be defined as domestic terrorism).

<sup>231</sup> See, e.g., *id.* § 32 (prohibiting destruction of aircraft or aircraft facilities"); *id.* § 37 (prohibiting violence at international airports); *id.* § 175 (prohibiting use, possession, or transport of biological weapons); *id.* § 229 (prohibiting use, possession, or transfer of chemical weapons); *id.* § 1114 (prohibiting killing of federal employees); *id.* § 1116 (prohibiting killing of foreign officials); *id.* § 1361 (prohibiting damage to government property); *id.* § 1362 (prohibiting damage to communication infrastructure); *id.* § 1992 (prohibiting violence against mass transportation systems); *id.* § 2332f (prohibiting bombings of government, public, or infrastructure facilities).

reach of § 2339B.<sup>232</sup> By limiting a civil cause of action for material support of domestic terrorism *only* to terrorism covered by § 2339A, lawsuits would necessarily require a causal nexus between the edge provider's support and the specific attack.<sup>233</sup>

Additionally, with § 230 fully intact, successful lawsuits would require the publishing edge provider to actually be complicit in hosting terrorist content.<sup>234</sup> Section 230 may prohibit holding edge providers vicariously liable for the content they host by prohibiting treating them as its publisher, but the statute does not apply to edge providers who are complicit in developing the content of the speech.<sup>235</sup> When an edge provider develops speech, they are not a computer service, they are a content provider, and thus they are directly liable for the speech itself.<sup>236</sup> Presently there is an enforcement gap in terrorism law: victims of international terror may seek redress against an edge provider that is actually complicit in perpetrating terrorism, but a domestic terror victim cannot.<sup>237</sup> Therefore, websites like Iron-March.org, where the owner actively cultivated an extremist userbase including members of Atomwaffen, cannot be pursued under current federal

---

<sup>232</sup> See, e.g., *Gonzalez v. Google, Inc.*, 282 F. Supp. 3d 1150 (N.D. Cal. 2017); *Pennie v. Twitter, Inc.*, 281 F. Supp. 3d 874 (N.D. Cal. 2017); *Cohen*, 252 F. Supp. 3d 140. The attacks in all three cases were carried out by ISIS-affiliated actors. *Gonzalez*, 282 F. Supp. 3d at 1153; *Pennie*, 281 F. Supp. 3d at 875; *Cohen*, 252 F. Supp. 3d at 142.

<sup>233</sup> See 18 U.S.C. §§ 2339A, 2339B. Section 2339A intrinsically does not face the same proximate cause issues that precluded previous lawsuits, which were foiled by the plaintiffs' inability to prove that the edge providers' provision of a platform for the terror organizations proximately led to members of those organizations carrying out attacks. See, e.g., *Fields III*, 881 F.3d 739, 749–50 (9th Cir. 2018). In *Fields*, Twitter could not be held liable because the attacker himself was not a Twitter user. *Id.* This is a problem likely unique to § 2339B—courts have recognized the distinction between § 2339B's more attenuated support connection and § 2339A's requirement of an actual terrorist act, finding that § 2339B necessitates a higher standard of proximate cause. See, e.g., *id.* Section 2339A, by contrast, can support the lower "reckless disregard" standard because the plaintiff need only allege a nexus between the material support and the *actual act*. *Holder v. Humanitarian Law Project*, 261 U.S. 1, 18–20 (2010). Plaintiffs like those in *Fields*, on the other hand, will inevitably face proximate causation problems because, by virtue of suing under § 2339B, they must prove that nexus based on an organization's use of a website. See *id.*; *Fields*, 881 F.3d at 750. Conversely, in a 2339A case predicated on a third party providing material support for the attack itself, a court could find a fact pattern which meets even stringent proximate cause standards. See *Fields*, 881 F.3d at 750.

<sup>234</sup> See 47 U.S.C. § 230(c); *infra* notes 235–251 and accompanying text.

<sup>235</sup> 47 U.S.C. § 230(c); see, e.g., *FTC v. Leadclick Media, LLC*, 838 F.3d 158, 176 (2d Cir. 2016) (holding that the CDA exists to protect edge providers from liability when performing a publisher's traditional editorial functions, but that protection does not extend to those who participate in developing unlawful content). The edge provider participating in publication to the extent that it develops speech ceases to be an "interactive computer service" and is instead considered an "information content provider." See, e.g., *Leadclick*, 838 F.3d at 176. The CDA does not afford immunity to information content providers. See *id.*

<sup>236</sup> 47 U.S.C. § 230(c); *Leadclick*, 838 F.3d at 174–75.

<sup>237</sup> See 18 U.S.C. § 2333 ("Any national of the United States injured by . . . international terrorism . . . may sue therefor . . .") (emphasis added).

law.<sup>238</sup> Amending § 2333 would bridge this gap without circumventing the core of the CDA.<sup>239</sup> Under such an amendment, websites like IronMarch.org, where the owner was complicit in hosting violent content including preparation for terror attacks, would be vulnerable to civil suit.<sup>240</sup> Facebook, however, would not be liable for hosting Ammon Bundy's multiple calls to arms and preparatory videos.<sup>241</sup> Though Bundy's underlying felonies fall under § 2339A, Facebook was not complicit in generating content with Bundy.<sup>242</sup> Facebook is therefore not a content provider, and claims against them for contributing to Bundy's terrorist actions would be barred by the CDA.<sup>243</sup>

Finally, amending § 2333 would encourage better practices by edge providers who do not actively participate in fostering or hosting domestic terrorism.<sup>244</sup> Litigation against edge providers for hosting foreign terrorist organizations, while unsuccessful, has brought political pressure to bear and has ultimately resulted in social media companies undertaking anti-terrorism measures on their platforms.<sup>245</sup> At present, most of these measures are centered around foreign extremism.<sup>246</sup> Should edge providers become potentially liable for providing material support to discrete domestic terror attacks, these beneficial anti-terror efforts might be applied in the domestic sphere as well.<sup>247</sup> Even public, nongovernmental pressure to crack down on white supremacy has yielded positive results: Twitter recently banned many accounts associated with white supremacy, and YouTube has demonetized or suspended several extremist accounts.<sup>248</sup> Although some commenters

---

<sup>238</sup> See *id.*; *Welcome to Hate Planet*, *supra* note 23. IronMarch.org's neo-Nazi owner Alisher Mukhitdinov is sometimes known by alias "Alexander Slavros." See *Illinois Woman*, *supra* note 127.

<sup>239</sup> See 18 U.S.C. § 2339A; *Leadclick*, 838 F.3d at 174 (citing the "core" of the CDA as "barring lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content").

<sup>240</sup> See 18 U.S.C. § 2339A; 47 U.S.C. § 230(c); *Leadclick*, 838 F.3d at 174.

<sup>241</sup> See 18 U.S.C. § 2339A; 47 U.S.C. § 230(c); Fenton, *supra* note 138 (reporting Ryan Bundy's statement of intent to "kill or be killed"); *Occupation Video*, *supra* note 139 (publishing call to arms and publicizing commencement of the occupation).

<sup>242</sup> See 18 U.S.C. § 2339A (providing no remedy where there is no material support).

<sup>243</sup> See *id.*

<sup>244</sup> See *id.*; *infra* notes 245–251 and accompanying text.

<sup>245</sup> Ali Breland, *Facebook, Twitter, YouTube Detail Fight Against Extremists at Senate Hearing*, THE HILL (Jan. 1, 2018) <http://thehill.com/policy/technology/369378-facebook-twitter-and-youtube-detail-fight-against-extremists-during-senate> [<https://perma.cc/E6CB-EVSS>] (discussing Facebook's recent attempts to address terrorist content on its platform, including banning extremist content and sharing technologies and data with other tech companies to prevent reuploading of that content).

<sup>246</sup> See *id.*

<sup>247</sup> See *id.*

<sup>248</sup> Kitty Donaldson & Joshua Brustein, *Twitter Bans Some White Supremacists and Other Extremists*, BLOOMBERG NEWS (Dec. 19, 2017), <https://www.fin24.com/Tech/Companies/twitter->

argue these actions alone are evidence of chilled speech, edge providers are free to respond to free market pressure as they deem necessary.<sup>249</sup> Ultimately, amending § 2333 to permit a very narrow subset of cases, to be pursued only when the edge provider actually develops speech, will disincentivize complicity in domestic terrorism while leaving the CDA itself intact.<sup>250</sup> A very narrow path to justice for victims of domestic terrorism will not dramatically alter a tech company's cost-benefit calculations, but sealing this open box of bad intent, bad players, and bad technology may, in the end, save lives.<sup>251</sup>

## CONCLUSION

White nationalist and neo-Nazi violence has accounted for dozens of deaths in recent years, impacting not only the lives of those directly affected, but also the public and political discourse about terrorism and extremism. The Internet's concurrent expansion into Americans' lives to the point of near-total ubiquity plays a critical role in this discussion, as social media allows for people with fringe viewpoints to connect, converse, and ultimately radicalize. That radicalization can and often does result in violence, and that violence often takes the form of domestic terrorism.

The federal framework for prosecuting domestic terrorism is shaky at best, and the added shield of § 230 of the CDA seemingly eliminates any possibility of prosecuting or holding tech companies liable for the content their platforms host, even when that content is directly tied to domestic terrorism. This is not necessarily a bad thing, as the Internet ecosystem has flourished under minimal regulation, and creating liability for hosting content would stymie, if not outright extinguish, that growth. But growth uninhibited by

---

bans-some-white-supremacists-and-other-extremists-20171219 [https://perma.cc://78TT-TU9C] (reporting Twitter's banning of several white supremacist accounts, including high profile individuals and organizations); Valentina Palladino, *Google Now Actively Works Against Extremist YouTube Videos*, ARSTECHNICA (June 19, 2017), <https://arstechnica.com/information-technology/2017/06/google-now-actively-works-against-extremist-youtube-videos> [https://perma.cc/KT5X-RS26] (reporting YouTube's recently implemented policy to eliminate advertising revenue for extremist and hateful content).

<sup>249</sup> See, e.g., Thomas Kadri, *Speech vs. Speakers: Twitter's New Rules About Extremist Speech Blur the Lines Between People and Words*, SLATE (Jan. 18, 2018), <https://slate.com/technology/2018/01/twitters-new-rules-blur-the-line-between-extremists-speakers-and-their-speech.html> [https://perma.cc/ACR8-MKDV] (arguing that Twitter's recent banning of extremist user accounts, versus individually offensive tweets, shifts the focus of content moderation from "speech" to "speaker" and risks chilling speech).

<sup>250</sup> See 18 U.S.C. § 2333 (permitting civil suit currently only in cases of foreign terrorism); 47 U.S.C. § 230(c).

<sup>251</sup> See Citron, *supra* note 212 (asserting that the Internet, like any forum for discussion such as a workplace, home, or coffee shop, does not merit special speech protections or exemptions from tort, criminal, or civil rights laws).

consideration for human cost is not morally or politically sustainable, and lawmakers face an impending balancing act between disregarding safety or cutting the Internet off at its knees. Thus far, they are leaning towards the latter.

Rather than passively allowing terrorism to fester on websites that court extremist content, or worse, taking drastic steps such as gutting the CDA, Congress should amend 18 U.S.C. § 2333 to permit victims of domestic terrorism to file civil suits against edge providers who are complicit in providing material support to acts of terror. Such a moderate solution would create only minor waves, forcing liability onto edge providers whose actions proximately cause harm, but without the collateral damage to tech companies who do not. Liability can be an effective deterrent, and when the grounds for suit are sufficiently narrow, the risk of tech companies overcorrecting is just as slim.

EMILY B. TATE

