IS THE DOMESTIC TERRORISM ATTACK ON THE CAPITOL AMERICA'S CHRISTCHURCH MOMENT? AN OPPORTUNITY FOR MORE CLARITY WITH THE COMMUNICATIONS DECENCY ACT AND MORE ACCOUNTABILITY FOR INTERNET PLATFORMS

*Megan Black**

I. INTRODUCTION

On the day that Congress counted the electoral votes to officially declare President Joseph R. Biden the 46th President of the United States, Make America Great Again ("MAGA") supporters marched into the Capitol, destroyed and stole property, endangered Congressmembers, and prevented the electoral vote from proceeding, all while streaming and posting their activity on social media.[1] While these acts of domestic terrorism captured the attention of the global community, former President Donald Trump ("Trump") continued to incite his supporters via Twitter and Facebook throughout the day while continuing to challenge the legitimacy of the voting process.[2]

* J.D. Candidate, Seton Hall University School of Law, 2022. Bachelor of Arts in Communications and Public Service from the University of Pennsylvania, 2015. I am grateful to Professor David Opderbeck for his guidance in writing, to Professor Charles Sullivan and Professor Michael Coenen for their time discussing potential topics, and to Hannah Teller, my comment editor, and the rest of the Journal team for helping throughout the drafting and editing processes. I would also like to thank my parents, sister, and friends for their support throughout this experience.

[1] *See* Shawn McCreesh, *What the MAGA Mob at the Capitol Had to Say for Itself*, THE NEW YORKER (Jan. 6, 2021), https://nymag.com/intelligencer/2021/01/what-the-maga-mob-at-the-capitol-had-to-say-for-itself.html; Julian Borger, *Maga Mob's Capitol Invasion makes Trump's Assault on Democracy Literal,* THE GUARDIAN (Jan. 7, 2021), https://www.theguardian.com/us-news/2021/jan/06/us-capitol-trump-mob-election-democracy.

[2] Brakkton Booker, *House Democrats Use Trump's Own Words To Argue He Showed No Remorse After Attack,* NPR (Feb. 11, 2021), https://www.npr.org/sections/trump-impeachment-trial-live-updates/2021/02/11/967034292/house-democrats-use-trumps-own-words-to-argue-he-showed-no-remorse-after-attack.

Trump even released a short video asking rioters to leave.[3] In this video, however, Trump told those on the Capitol "we love you, you're special" and continued to assert that he had won the election saying, "I know your pain, I know you're hurt. We had an election that was stolen from us. It was a landslide election, and everyone knows it. Especially the other side. But you have to go home now. We have to have peace."[4] Many commentators point to rampant evidence of the Trump administration's aggression and misinformation on social media platforms and accordingly blame social media companies for not doing more to police their platforms aside from labeling Trump's posts.[5]

Contrarily, after a gunman, thought to be an Australian white nationalist, shared a hate-filled manifesto online and used Facebook to livestream the mass murder of fifty people at two Mosques in Christchurch, New Zealand, the Australian government passed legislation that imposes huge fines for social media companies and jail time for their executives if they do not rapidly remove "abhorrent violent material" from their platform.[6] The Australian government took swift and clear action to ensure that terrorism will not be streamed on social media without consequences again.

Unlike Australia, U.S. Government leaders did not take any immediate legislative steps, but social media companies took action, banning Trump temporarily from Twitter, Facebook, and Instagram.[7] These platforms also removed some of his statements.[8] Additionally, YouTube stated that it would not tolerate violence on its sites and claimed to remove multiple livestreams that showed the rioters in the Capitol carrying

[3] Travis Caldwell, *Trump's 'We Love You' to Capitol Rioters is More of the Same*, CNN (Jan. 7, 2021), https://www.cnn.com/2021/01/07/politics/trump-history-comments-trnd/index.html.

[4] *Id.*

[5] Kate Conger et. al., *Twitter and Facebook Lock Trump's Accounts After Violence on Capitol Hill*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2021/01/06/technology/capitol-twitter-facebook-trump.html.

[6] Damien Cave, *Australia Passes Law to Punish Social Media Companies for Violent Posts,* N.Y. TIMES (Apr. 3, 2019), https://www.nytimes.com/2019/04/03/world/australia/social-media-law.html.

[7] Conger, *supra* note 5.

[8] Caldwell, *supra* note 3.

firearms.[9] Whether it is viewed as admirable or too little, too late, the varied and independent actions taken by social media companies are not sufficient. Codified legal standards are needed, initially to identify the type of content that can and cannot remain online, and subsequently to determine the liability of social media companies for failing to meet such initial benchmarks. Without legislative guideposts, platforms can rely solely on company-specific policies, which prevent individuals from having uniform expectations about the type of material that is acceptable on the platforms. This is where the Communications Decency Act ("CDA") could come into play.

The CDA, 47 U.S. Code § 230, provides legal protection against liability for websites that have user-generated content.[10] Congress passed this act with the intention of promoting broad Internet growth and creativity.[11] Currently, the CDA provides extensive flexibility for social media platforms to avoid accountability for the behavior of others in the name of ensuring the development of the Internet, modern technologies, and online competition. The elements required for Section 230(c) immunity are: (1) that the defendant is a provider or user of an interactive computer service; (2) that the asserted claims treat the defendant as the publisher or speaker of the information; and (3) that the information is provided by another information content provider.[12] Based on how platforms evolved, the political environment, the need for privacy, and the reliance people have on the content posted on the platforms, Congress must establish greater accountability for platforms.

First, this comment conducts a comparative analysis of the Australian Sharing Abhorrent Violent Material Criminal Code Amendment and the CDA. In comparing these laws, the comment evaluates the context in which they arose, the intent of the legislation, and the subsequent application of the laws. The Australian law is the focus of comparison for the CDA because it is a piece of recent legislation that received a number of critiques that provide a good starting point for any proposed changes to

9 Conger, *supra* note 5.

10 47 U.S.C.A § 230(c).

11 47 U.S.C.A § 230(b).

12 47 U.S.C.A § 230(c).

the CDA.

This comment then evaluates the problem with how the CDA is operating today. It further considers newer issues that arose in the context of online hate, such as doxing, as well as government action in this space, including the Trump Administration's Executive Order about social media censorship, the Fight Online Sex Trafficking Act ("FOSTA"), and the Stop Enabling Sex Traffickers Act ("SESTA").

The goal of this analysis is to highlight why there needs to be a change in the immunity provided to online platforms. The Internet has evolved since Congress passed the CDA, and it is time for codified standards that articulate what online content is unacceptable and what actions platforms need to take to avoid liability when the content on their platform does not meet the standards. This article concludes with potential pathways for change to create greater liability for platforms and more consistency for the quality of online content.

II. BACKGROUND

Seven out of ten Americans use social media to follow the news, share personal content, entertain themselves, and connect with others.[13] This reliance on social media for information allows Internet platforms to shape and steer public discourse.[14] When the Pew Research Center asked which platforms respondents use on a daily basis, researchers found preferences for the following platforms: Facebook (74%), Instagram (63%), Snapchat (61%), YouTube (51%), and Twitter (42%).[15]

Despite the wide use of social media, 64% of Americans say social media has a mostly negative effect on the country.[16]

---

[13] Natalie Annette Pagano, Comment, *The Indecency of the Communications Decency Act § 230: Unjust Immunity for Monstrous Social Media Platforms*, 39 PACE L. REV. 511, 512 (2018).

[14] Annemarie Bridy, *Remediating Social Media: A Layer-Conscious Approach*, 24 B.U. J. SCI. & TECH. L. 193, 195 (2018).

[15] Andrew Perrin & Monica Anderson, *Share of U.S. Adults Using Social Media, Including Facebook, is Mostly Unchanged Since 2019*, PEW RESEARCH CENTER (Apr. 10, 2019), https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/ (providing a breakdown of social media use by platform and demographic lines).

[16] Brooke Auxier, *64% of Americans Say Social Media Have a Mostly Negative*

Notably, this view varies based on political affiliation and age, with more young adults saying social media has a positive impact.[17] YouTube and Facebook are the most widely used online platforms, and as a result have a broader user base that is more representative of the American population as a whole when compared to sites used less frequently like Twitter, Pinterest, Instagram, and LinkedIn.[18] But Instagram has a wide number of users as well, with young adults and women most likely to say that they use it, and there is a range of varying age groups using the platform: 75% of adults aged 18 to 24, 57% of adults 25 to 29 years old, 47% of adults 30 to 49 years old, 23% of adults 50 to 64 years old, and 8% of adults 65 years and older.[19] Instagram is not a top media site for news, with only 14% of adults saying they get news on the platform, similar to the number of adults who get news from Twitter (17%); notably, Instagram and Twitter are used significantly less for news content than Facebook (52%) and YouTube (28%).[20]

A year-over-year analysis found that social media use by U.S. adults largely did not change despite issues with privacy, fake news, and censorship on social media.[21] Facebook remains one of the most widely used social media sites among adults in the U.S.[22] Almost seven-in-ten adults (69%) say that they use Facebook, while 73% of adults report using YouTube, making it the only other online platform measured that matches Facebook's reach.[23] But other online platforms, like Instagram and Snapchat, have cultivated larger followings with younger social media users.[24]

Effect on the Way Things Are Going in the U.S. Today, PEW RESEARCH CENTER (Oct. 15, 2020), https://www.pewresearch.org/fact-tank/2020/10/15/64-of-americans-say-social-media-have-a-mostly-negative-effect-on-the-way-things-are-going-in-the-u-s-today/.

17 Auxier, *supra* note 16.

18 *Social Media Fact Sheet*, PEW RESEARCH CENTER (April 7, 2021), https://www.pewresearch.org/Internet/fact-sheet/social-media/.

19 Brooke Auxier, *8 Facts About Americans and Instagram*, PEW RESEARCH CENTER (Oct. 21, 2020), https://www.pewresearch.org/fact-tank/2020/10/21/8-facts-about-americans-and-instagram/.

20 Auxier, *supra* note 16.

21 Perrin, *supra* note 15.

22 Perrin, *supra* note 15.

23 Perrin, *supra* note 15.

24 Perrin, *supra* note 15.

Despite the lack of trust many social media users have for the platforms, social media is part of the daily routine of many Americans, with roughly 70% of Facebook users and around 60% of Instagram users visiting the platforms at least once a day.[25] Importantly, social media encompasses a broad array of online platforms and is not limited to websites traditionally thought of as social media like Facebook and Twitter.[26] Any website that possesses a comment section or allows for readers to respond and thus hosts third party content could be considered social media.[27]

A 2019 survey from the Pew Research Center found that 55% of Americans believe technology companies have too much influence and power.[28] Further, a majority of Americans (72%) think that social media websites intentionally censor political viewpoints the platform finds objectionable.[29] While 66% of Americans generally believe social media websites have a responsibility to remove offensive content from platforms, few Americans have confidence in the ability of the social media company to determine which offensive content should be removed from the platform.[30] The greatest response was from 45% of Americans who decided they possessed "not too much" confidence in the platforms, while 24% of Americans have no confidence that the sites will adequately determine what is offensive and thus should be removed.[31] Further, almost half of those surveyed, 48%, said it was "hard to know" what others might perceive as offensive content that should be removed.[32]

---

[25] *Social Media Fact Sheet*, PEW RESEARCH CENTER (June 12, 2019), https://www.pewresearch.org/Internet/fact-sheet/social-media/.

[26] George Fishback, *How the Wolf of Wall Street Shaped the Internet: A Review of Section 230 of the Communications Decency Act*, 28 TEX. INTELL. PROP. L.J. 275, 280 (2020).

[27] *Id.*

[28] Carroll Doherty & Jocelyn Kiley, *Americans Have Become Much Less Positive About Tech Companies' Impact on the U.S.*, PEW RESEARCH CENTER (July 29, 2019), https://www.pewresearch.org/fact-tank/2019/07/29/americans-have-become-much-less-positive-about-tech-companies-impact-on-the-u-s/.

[29] *Id.*

[30] John Laloggia, *U.S. Public has Little Confidence in Social Media Companies to Determine Offensive Content*, PEW RESEARCH CENTER (July 11, 2019), https://www.pewresearch.org/fact-tank/2019/07/11/u-s-public-has-little-confidence-in-social-media-companies-to-determine-offensive-content/.

[31] *Id.*

[32] *Id.*

This research indicates that even though many Americans are comfortable using social media in their daily lives, they do not trust the platforms to adequately monitor content. Therefore, a nationally mandated standard is necessary.

III. DIFFERENT APPROACHES

A. *Background*

1. Australia

Since Australia has more restrictive legislation that attempts to hold social media companies accountable, it will serve as a comparison point for how the CDA could evolve. The violent acts in Christchurch provided a moment of reckoning for the Australian legislature, which took the violence as an opportunity to create mandated community norms for online content and forced accountability on the platforms.

Prior to the passage of the *Sharing of Abhorrent Violent Material Act 2019* ("SAVMA"), which amended the criminal code, Australia relied on inconsistent judge-made law to define the scope of intermediary liability for third party conduct.[33] For example, the Supreme Court of Victoria held that Google is a publisher of search results because employees possess skill and expertise for the purpose of creating a search engine and Google intends its search engines to publish material on the Internet in response to a search.[34] By contrast, the Supreme Court of New South Wales found Google is not a publisher because search results are generated by an algorithm, rather than human activity.[35] Although the New South Wales court agreed with the Supreme Court of Victoria that people created the algorithms, it did not find the level of human usage to be sufficient to establish

[33] Brett G. Johnson, *Innovation in Media and Entertainment Law: Symposium Article: Beyond Section 230: Liability, Free Speech, and Ethics on Global Scale Networks*, 2 BUS., ENTREPRENEURSHIP & TAX L. REV. 274, 295 (2018).

[34] The Supreme Court of Victoria is the highest court in Victoria dealing with the most serious civil and criminal cases within the State of Victoria. *How The Court Works*, SUPREME COURT OF VICTORIA, https://www.supremecourt.vic.gov.au/about-the-court/how-the-court-works (last visited Oct. 2, 2021); Johnson, *supra* note 33, at 295.

[35] Johnson, *supra* note 33, at 295.

Google as a publisher.[36] Further, the Supreme Court of the Australian National Territory—located in the capital of Canberra—found a website smaller than Google, which encouraged users to make defamatory posts, to be a publisher under Australian law and liable for the posts.[37] Australian case law does not establish a clear line between global intermediaries and local small-time intermediaries for the purposes of liability.[38] SAVMA matches or exceeds other democracies' attempts to punish multinational technology companies for third party user-generated content.[39] This legislation establishes new offenses by criminalizing a list of "abhorrent violent material," and creates greater liability for platforms failing to take down content by establishing punitive measures, such as imprisonment and fines up to 10 percent of the company's annual profit.[40]

Australia's Attorney General at the time, Christian Porter, expected the act to "send a clear message that the Australian government expects the providers of online content and hosting services to take responsibility for the use of their platforms to share abhorrent violent material."[41] The conversation surrounding the legislation focused on the length of time the Christchurch attack streamed and the length of time it took to contain the streaming and take it down.[42] Legislators also focused on holding social media companies more accountable for any violent material on the platforms.[43] This legislation passed in early April after the attack in mid-March with both houses passing the legislation within 24 hours, and it received general approval from all legislators.[44]

---

36 Johnson, *supra* note 33, at 295.

37 Johnson, *supra* note 33, at 295–96.

38 Johnson, *supra* note 33, at 296.

39 Cave, *supra* note 6.

40 *See* Evelyn Douek, *Australia's New Social Media Law is a Mess*, LAWFARE (Apr. 10, 2019), https://www.lawfareblog.com/australias-new-social-media-law-mess#; Cave, *supra* note 6. Note the provisions of SAVMA will be discussed further in General Law Provisions.

41 *Id.*

42 *Id.*

43 *Id.*

44 *Id.*

2. Potential European Influences

The European Union, through the European Commission, outlined recommendations that members should take "to effectively tackle illegal online content," specifically advocating for online platforms to be more responsible in content governance along a few key metrics.[45] These metrics include creating clear "notice and action" procedures; creating efficient tools and proactive technologies; safeguarding fundamental rights; working with small companies; and cooperating with authorities.[46] Another potential source of inspiration is France, which, in the wake of the attack on Charlie Hebdo magazine, enacted sweeping legislation that curtailed freedom of movement and expression.[47] Part of this legislation allowed the French government to block websites that "incite or glorify" terrorism without receiving previous judicial authority.[48] This need for permission can curtail free expression while failing to adequately address the terrorism issue that it aims to prevent.[49] The Australian regulation also follows in the footsteps of "The German Act to Improve the Enforcement of the Law in Social Networks" (NetzDG), which requires social media networks and service providers to take down "manifestly unlawful" content within 24 hours or the provider can face large fines reaching €50

---

[45] *Illegal Content on Online Platforms*, EUR. COMM'N, https://ec.europa.eu/digital-single-market/en/illegal-content-online-platforms (last visited Oct. 2, 2021).

[46] *Id.*

[47] Eglantine Stauton, *France, 'Cradle of Liberty,' Struggles to Balance Anti-terrorism Law and Rights*, THE CONVERSATION (May 7, 2015), https://theconversation.com/france-cradle-of-liberty-struggles-to-balance-anti-terrorism-law-and-rights-41412; *see also* Dan Bilefsky & Maïa de la Baume, *Terrorists Strike Charlie Hebdo Newspaper in Paris, Leaving 12 Dead*, N.Y. TIMES (Jan. 7, 2015), https://www.nytimes.com/2015/01/08/world/europe/charlie-hebdo-paris-shooting.html (sharing that the terrorist attack by Muslim extremists on Charlie Hebdo magazine left twelve people dead including editors, cartoonists, and police men in one of the deadliest attacks in postwar France that was thought to be inspired by magazine's inclusion of cartoons satirizing Muslim community).

[48] Press Release, Human Rights Watch, France: Counterterrorism Bill Threatens Rights (Oct. 9, 2014) (on file with author), https://www.hrw.org/news/2014/10/09/france-counterterrorism-bill-threatens-rights#.

[49] *Id.*

million.[50] Both laws provide examples of limiting the types of content shared online and attempting to punish individuals for sharing the banned content.

3. United States of America

Congress wanted to promote free speech, self-regulation, and the rise of Internet enterprises with the CDA.[51] Congress enacted the CDA during the early days of the Internet to protect interactive computer service providers from civil liability for the actions of a third party by ensuring that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another content provider."[52]

Legislators intended the CDA to encourage provider awareness of the content featured on their services and to help address emerging problems concerning issues with the quality of information online and the struggles of parents to limit children's exposure to adult content, such as pornography.[53] Specifically, the CDA made it illegal to "knowingly send to or show minors obscene or indecent content online."[54] Congress tacked this measure onto the Telecommunications Act, which provided a major update to a sixty-year-old law, seemingly to address new technological advancements like the Internet.[55] Congress also wanted to protect Internet service providers

[50] Evelyn Douek, *Germany's Bold Gambit to Prevent Online Hate Crimes and Fake News Takes Effect*, LAWFARE (Oct. 31, 2017), https://www.lawfareblog.com/germanys-bold-gambit-prevent-online-hate-crimes-and-fake-news-takes-effect (noting "there are exemptions for certain platforms: nonprofits, publishing and journalism enterprising and platforms designed to enable individual communication (such as messaging apps) or the dissemination of specific content (such as dating websites)" as well as "networks with fewer than two million registered German users").

[51] Michal Lavi et al., *Do Platforms Kill?*, 43 HARV. J. L. PUB. POL'Y 477, 511 (2020); *see also* 47 U.S.C.A § 230(b).

[52] Orly Lobel et al., *The Law of the Platform*, 101 MINN. L. REV. 87, 144 (Nov. 2016).

[53] Bridy, *supra* note 14, at 206–07.

[54] *CDA 230: Legislative History*, ELECTRONIC FRONTIER FOUNDATION: ISSUES, https://www.eff.org/issues/cda230/legislative-history (last visited Sept. 14, 2021) [hereinafter EFF].

[55] *Id.*

("ISPs") who feared liability for defamation by removing objectionable content as a publisher under the CDA.[56] Therefore, Congress added an immunity provision as an amendment that prevented any provider from being treated as the publisher or speaker of third party content and excused them from liability.[57] This context of protecting minors from indecent and explicit material disappeared because the United States Supreme Court struck down the anti-indecency sections of the CDA for violating the First Amendment.[58] The First Amendment establishes the right to free speech, but that right is not absolute.[59] Traditionally, obscenity, which is the type of content that the CDA aimed to prohibit, is not protected by the First Amendment.[60] However, the Court is often stuck between impermissible obscenity and content on sexual material that is protected by the First Amendment.[61] To address this distinction, the Supreme Court established a test in *Miller v. California*[62] to distinguish obscene material from sexual material protected by the First Amendment by evaluating any potential value or offense of the content.[63] Despite this guidance, well-intended legislation

---

56 Mark A. Lemley, *Digital Rights Management: Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 102 (2007).

57 *See* Lemley, *supra* note 56, at 102–03; EFF, *supra* note 54.

58 Bridy, *supra* note 14, at 208; *see also* Reno v. Am. C.L. Union, 521 U.S. 844, 858, 881 (1997) (holding "the CDA places an unacceptably heavy burden on protected speech," thus making the provisions concerning Internet provider liability for indecent and patently offensive content material unconstitutional).

59 Miller v. California, 413 U.S. 15, 23 (1973) (establishing the First Amendment is not absolute); *see also* Rebecca Jakubcin, *Reno v. ACLU: Establishing a First Amendment Level of Protection for the Internet*, 9 U. FLA. J. L. & PUB. POL'Y, 287, 288 (1998).

60 *Miller*, 413 U.S. at 23 (stating "obscene material is unprotected by the First Amendment" and establishing the First Amendment is not absolute); *see also Obscenity*, THE DEPARTMENT OF JUSTICE: SUBJECT AREAS, https://www.justice.gov/criminal-ceos/obscenity#:~:text=Obscenity%20is%20not%20protected%20under,obscenity%20laws%20are%20criminal%20offenses.&text=(For%20more%20information%2C%20see%20Citizen's,of%20obscene%20matter%20to%20minors (last visited Sept. 14, 2021).

61 61 AM. JUR. 3d. 51 *Proof of Facts* § 4 (2001).

62 Miller v. California, 413 U.S. 15 (1973).

63 *Id.* at 24 establishing the three-prong test, which states:

> (a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest . . . (b) whether the work depicts

can still miss the mark and result in court action against potential First Amendment violations, as evidenced by the lawsuit challenging the CDA.

Immediately after the Telecommunications Act was signed into law, twenty plaintiffs filed suit against the indecency provision, resulting in *Reno v. American Civil Liberties Union*.[64] The Court found that the anti-indecency parts of the CDA were too vague given that they regulated the content of speech.[65] The terms "indecent" and "patently offensive" lacked a definition, which created uncertainty around potential violations.[66] Further, the Court found that the open-ended coverage of the CDA was unprecedented and distinct from prior decisions that upheld limitations on indecent content when the regulation specifically targeted commercial speech or commercial entities.[67] The Internet presented a distinct technological concern because it is highly accessible and hosts a variety of platforms and resources.[68] This distinction meant the CDA's ambiguous restrictions concerning obscene, offensive, or indecent material created an overbroad standard that reached protected speech.[69]

The Court also concluded that the CDA, in an attempt to prevent minors from accessing potentially harmful content, unacceptably suppressed speech that adults have a constitutional right to receive and address.[70] In applying the test established in

> or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

64 Reno v. Am. C.L. Union, 521 U.S. 844, 861 (1997).

65 *Id.* at 874–75 (finding that while the government has a compelling interest in protecting children, the solution of suppressing large amount of speech is not sufficiently narrowly tailored to pass strict scrutiny); *see generally* R.A.V. v. St. Paul, 505 U.S. 377, 395 (1992) (providing more information about First Amendment analysis while asserting the First Amendment prohibits content-based regulation of speech unless the regulation passes strict scrutiny, meaning it is narrowly tailored to serve a compelling government interest.)

66 *Reno*, 521 U.S. at 871.

67 *Id.* at 877.

68 *See* Jennifer J. Lee, *The Internet and First Amendment Values: Reno v. ACLU and the Democratization of Speech in the Marketplace of Ideas*, 22 COLUM.-VLA J. L. & ARTS 61, 67 (1997).

69 *See id.*

70 *Reno*, 521 U.S. at 874.

Miller, the Court found the CDA indecency provision failed because the "vague contours" of the statute "unquestionably silence[] some speakers whose messages would be entitled to constitutional protection."[71] The Court also referenced precedent establishing "[s]exual expression which is indecent but not obscene is protected by the First Amendment."[72] The Court only struck down the indecency provisions, leaving the immunity provision of the Telecommunications Act intact.[73] This made the immunity provision more general than initially intended, and platforms use that provision to avoid liability for not removing content from their sites.[74] This immunity is further expanded by the courts because judges are more prone to decide close cases in favor of immunity for the platform.[75]

Congress delineated the research findings that inspired the creation of the CDA. First, the creation of the Internet and other interactive computer services greatly increased the availability of educational and informational resources to Americans.[76] Second, the services provide users with a great amount of control over the content they consume.[77] Third, these new technologies provide a forum for diversity, development, and discourse in culture, politics, and intellectual ideas.[78] Fourth, without government regulation, the Internet and related technologies flourished.[79] Finally, users are becoming increasingly reliant on the new services for a number of educational, entertainment, cultural, and political uses.[80]

---

71 *Id.* at 873–74 (finding the CDA exceeded the narrower "sexual conduct" restraint of *Miller* for placing further limitations on content excluding "organs" and "excretory activities," and failed to account for contemporary community standards as well as potential literary, artistic, political, or scientific value as indicated by *Miller*).

72 *Id.* (citing Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989)).

73 EFF, *supra* note 54.

74 Bridy, *supra* note 14, at 208.

75 Bridy, *supra* note 14, at 212.

76 47 U.S.C.A § 230 (a).

77 *Id.*

78 *Id.*

79 *Id.*

80 *Id.*

B. *General Law Provisions*

SAVMA sets out obligations of ISPs, content service providers ("CSP"),[81] and hosting service providers ("HSP") when abhorrent violent material or conduct is present on their site.[82] Abhorrent violent material is audio, visual, or audiovisual material, that records or streams abhorrent violent conduct of one or more persons that a reasonable person would view as offensive.[83] This material must be produced by one or more individuals, each of whom engaged in the conduct, conspired to engage in the conduct, aided or knowingly engaged in the conduct, or attempted to engage in the conduct.[84] It is insignificant if the material was altered or created outside of Australia.[85] Abhorrent violent conduct includes terrorist acts, murder, attempted murder, torture, rape, and kidnapping.[86]

The provider commits an offense under SAVMA for failure to notify if abhorrent violent material or conduct appears on the site.[87] Specifically, an offense is committed if the person: (1) is an ISP; or (2) provides a content or hosting service; and (3) is aware that the service can be used to access abhorrent violent material or conduct; and (4) does not submit details of the violent material to Australian Federal Police within a reasonable time after gaining awareness of the material's existence.[88] It is immaterial if the content or hosting service is within or outside Australia.[89]

Content and service providers also face liability for failing to remove or continuing to host the abhorrent violent material, meaning the material must not be "accessible to any of the end-

81 For the purpose of a CSP, "a person does not provide a content service merely because the person supplies a carriage service that enables material to be accessed" and "a person does not provide a content service merely because the person provides a billing service, or a fee collection service, in relation to a content service." *Criminal Code Amendment (Sharing of Abhorrent Violent) Act 2019* (Cth) sch 1 (Austl.).

82 *Id.*

83 *Id.*

84 *Id.*

85 *Id.*

86 *Id.*

87 *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth) sch 1 (Austl.).

88 *Id.*

89 *Id.*

users using the service."[90] An individual commits an offense when: (1) he provides a content or hosting service; (2) the service can be used to access abhorrent violent material; and (3) he does not enable the quick removal of the material from the service.[91] The person is only liable for not removing abhorrent violent material unless the material is reasonably capable of being accessed within Australia.[92] Again, it is immaterial whether the service is provided from within or outside Australia.[93] The requisite intent for this offense is recklessness.[94]

Should an individual not take down the content from the content or hosting service, the eSafety Commissioner can issue a written notice only if a specified service could be used to access the abhorrent violent material.[95] The commissioner is not required to observe procedural fairness to provide notice, but the commissioner must provide a copy of the notice to the service provider.[96] If notice is provided and the prosecution proves that the service could be used to access the material, then it must be presumed that the person was reckless.[97] But, the presumption can be rebutted if the person shows that there was a reasonable possibility the person was not recklessly accessing the material when the notice was issued.[98] This same presumption applies as to whether the material is abhorrent violent material; in other words, it is presumed when notice was given that the provider was reckless as to the violent abhorrent material unless the provider rebuts this presumption.[99] This again applies whether the material or platform is in or out of Australia.[100]

The CDA has fewer guidelines than SAVMA about what activities are prohibited and what is required of providers. The

90 *Id.*

91 *Id.*

92 *Id.*

93 *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth) sch 1 (Austl.).

94 *Id.*

95 *Id.*

96 *Id.*

97 *Id.*

98 *Id.*

99 *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth) sch 1 (Austl.).

100 *Id.*

CDA outlines the findings discussed above, policy initiatives, an obligation concerning preventing children from accessing obscene material, immunity for providers, and areas of law that are not impacted by the CDA.[101] The lack of clear guidelines enabled a large amount of court interpretation defining the scope and boundaries of the different provisions of the CDA, which is especially true in the immunity space.[102] This has led to broad permissions unless there is a specific content type, such as sex trafficking, that the legislation determined did not qualify for the broad immunity.[103] Court interpretation is especially impactful for cases challenging the meaning of "publisher" under the CDA as there is no definition within the CDA.[104]

The CDA outlines the policies of the U.S. when it comes to the Internet and new technology growth and what the CDA is trying to protect and enable. First, the CDA aims to promote the creation and "continued development of the Internet and other interactive computer services and other interactive media."[105]

---

101 47 U.S.C.S. § 230.

102 VALERIE BRANNON, CONG. RSCH. SERV., LSB10306, LIABILITY FOR CONTENT HOSTS: AN OVERVIEW OF THE COMMUNICATION DECENCY ACT (2019).

103 Madeline Byrd & Katherine Strandburg, *CDA 230 for a Smart Internet*, 88 FORDHAM L. REV. 405, 408–09 (2019) ("Many cases have tested the scope of "publisher" activities, with results holding, for example, that CDA 230 immunizes decisions about what to post; nonsubstantive editing; reformatting of fonts, colors, and the like; and re-presentation of information in the form of star ratings or maps.").

104 *Id.*, at n. 22 comparing the holdings concerning the CDA from different circuits,

> Marshall's Locksmith Serv. Inc. v. Google, LLC, 925 F.3d 1263, 1269–71 (D.C. Cir. 2019) (finding CDA immunity even where Google put the advertisements into a map format); Kimzey v. Yelp! Inc., 836 F.3d 1263, 1269–70 (9th Cir. 2016) (finding CDA immunity even where Yelp! took reviews from a different website and added a star rating); O'Kroley v. Fastcase, Inc., 831 F.3d 352, 355 (6th Cir. 2016) (finding CDA immunity even where Google had performed some "automated editorial acts on the content, such as removing spaces and altering font" and "kept the search result up even after [the plaintiff] complained about it"); Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 416 (6th Cir. 2014) ("The CDA expressly bars '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.").

105 47 U.S.C.A § 230(b)(1).

Second, the provisions preserve the Internet's free market by not imposing unnecessary federal or state regulations.[106] Third, the CDA aims to promote new technology development to allow for improved user control over the information available on the Internet and through other interactive services.[107] Fourth, the provisions incentivize the creation and use of blocking and filtering technologies to allow parents to restrict their child's access to inappropriate material online.[108] Finally, the CDA allows for the enforcement of federal criminal laws to prevent and punish obscenity, stalking, and harassment via the computer.[109]

Further, the CDA establishes that interactive computer services providers[110] have an obligation to:

> at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.[111]

This imposes a minimal obligation on providers while offering protection from liability, however, it has no effect on criminal law, intellectual property law, communications privacy law, and

106 47 U.S.C.A § 230(b)(2).

107 47 U.S.C.A § 230(b)(3).

108 47 U.S.C.A § 230(b)(4).

109 47 U.S.C.A § 230(b).

110 "The term 'interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C.A § 230(f).

111 47 U.S.C.A § 230(d).

sex trafficking law.[112]

C. *Liability*

Australian case law establishing the line distinguishing the terms of liability for global intermediaries and local small-time intermediaries is unclear.[113] SAVMA matches or exceeds other democracies' attempts to punish multinational technology companies for the behavior of the third party users generating content.[114] The Attorney General at the time wanted the act to "send a clear message that the Australian government expects the providers of online content and hosting services to take responsibility for the use of their platforms to share abhorrent violent material."[115]

But SAVMA does offer a defense for content service providers and hosting services if the abhorrent violent material was accessible under certain conditions.[116] For example, there is no crime if the platform uses the violent material to help law enforcement either enforce an Australian law or a law of a foreign country or comply with monitoring as required by law.[117] There is also a defense if access to the violent material is necessary for court proceedings or to advocate for a change to a law, policy, or practice in Australian or foreign law as long as there is a reasonable connection between the content and the advocacy or the accessibility is necessary for the "development, performance, exhibition or distribution, in good faith, of an artistic work."[118] There are also exceptions if an individual is conducting medical, scientific, academic, or historical research and the accessibility is reasonable for the research purposes.[119]

Further, there is a defense if the content relates to a news or current affairs report that is for the benefit of the public and is

112 47 U.S.C.A § 230(e)(1)-(2), (4)-(5).

113 Johnson, *supra* note 33, at 296.

114 Cave, *supra* note 6.

115 Douek, *supra* note 40.

116 *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth) sch 1 (Austl.).

117 *Id.*

118 *Id.*

119 *Id.*

made by a professional such as a journalist.[120] Finally, public officials also have a defense as long as the material is connected to the performance of the official's duties or functions and it is reasonably related to the performance of the duties.[121] If utilizing one of these defenses, the defendant bears the burden of producing evidence.[122] Importantly, the defenses also extend to matters and things outside Australia. [123] Additionally, there is no violation of notification if the person "reasonably believes that details of the material are already known to the Australian Federal Police."[124] But, the burden is on the defendant to prove the reasonableness of the belief the police already knew. [125]

Compared to the approach taken by Australia and many other countries, the CDA is considered one of the most lenient laws because it only holds a platform liable when it "materially contribute[d]" to the creation of the user-generated content.[126] This model gives platforms a significant degree of control over user-generated content without making platforms take any legal responsibility for such content.[127] The Safe Harbor provision has the effect of limiting provider liability for users' illegal content while containing provisions enabling providers to remove illegal and offensive content from their platforms.[128]

D. *Immunity/Exceptions*

SAVMA does not apply to political communications, meaning the law does not apply "to the extent . . . that it would infringe any constitutional doctrine of implied freedom of political communication."[129] The choice to provide immunity for political communications could explain why the critiques of

120 *Id.*

121 *Id.*

122 *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth) sch 1 (Austl.).

123 *Id.*

124 *Id.*

125 *Id.*

126 Johnson, *supra* note 33, at 302.

127 Johnson, *supra* note 33, at 302.

128 Bridy, *supra* note 14, at 206.

129 *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (Cth) sch 1 (Austl.).

SAVMA focused on the obligations of platforms and ambiguities, instead of the rights of users. Unlike the U.S. Constitution, Australia's Constitution does not explicitly provide the right to free expression, instead, there is an implied freedom of political communication.[130] Therefore, the immunity provided seemingly protects the freedom of expression Australians are guaranteed.

Only featuring one exception for a type of content is a jarring difference compared to the immunity the CDA offers platforms. The CDA "protects social media platforms from nearly all lawsuits regarding content posted by third parties."[131] Further, the CDA's immunity provision encourages platforms to remove offensive material and participate as good citizens because the platform is not liable as an editor for taking that action.[132] Immunity also "promotes free speech and e-commerce because" providing a platform immunity nurtures the growth of the platform.[133]

"'Good Samaritan' blocking and screening of offensive material" assert that "[n]o provider or user of an interactive . . . service" will "be treated as the publisher or speaker of . . . information provided by another."[134] This means providers are not liable for any action taken in good faith to restrict material the platform values:

> obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[135]

---

130 *See Freedom of Information, Opinion and Expression*, AUSTRALIAN HUM. RIGHTS COMM'N: RTS. AND FREEDOMS, https://humanrights.gov.au/our-work/rights-and-freedoms/freedom-information-opinion-and-expression (last visited Oct. 2, 2021).

131 Pagano, *supra* note 13, at 513.

132 Frank Fagan, *Systemic Social Media Regulation*, 16 DUKE L. & TECH. REV. 393, 436 (2017–2018).

133 *Id.* at 436.

134 47 U.S.C.A § 230(c)(1).

135 47 U.S.C.A § 230(c)(2).

The immunity offered by the CDA creates a federal immunity for any cause of action that makes ISPs liable for information posted originally by a user of the service, meaning, courts cannot hear claims that frame the service provider as if it were the publisher of the content.[136] This law provides immunity in the form of civil liability to ISPs for the content third parties post or publish on the platforms.[137]

The provision prevents people from taking legal action to hold a service provider liable for exercising editorial functions, like deciding to publish, withdraw, postpone, or change content.[138] This is often seen as a double-prong of immunity because it immunizes the platform if it moderates content and if it chooses not to moderate content.[139] There are two rationales for immunity.[140] The first is to lower the cost of sifting through material to determine if a platform finds negative material, because of a fear the platform will not maintain the site if the cost is too high.[141] The second is to protect the freedom of expression for all by preventing frivolous takedowns of content.[142]

But this immunity is limited. While the CDA grants broad immunity to websites with user-generated content, "it does not apply to Internet sites that 'materially contribute'" to either the "branding or shaping" of the post or other unlawful content.[143] Courts generally utilize three criteria to determine if CDA immunity applies to an ISP.[144] Initially, courts evaluate if the defendant is "the provider or user of an 'interactive computer service'" ("ICS").[145] Courts allow a variety of online platforms to

136 Fishback, *supra* note 26, at 286.

137 Johnson, *supra* note 33, at 288.

138 Fishback, *supra* note 26, at 286.

139 James Grimmelmann, *The Virtues of Moderation*, 17 YALE J. L. & TECH. 42, 103 (2015).

140 Johnson, *supra* note 33, at 289.

141 Johnson, *supra* note 33, at 289.

142 Johnson, *supra* note 33, at 289.

143 Lobel, *supra* note 52, at 145.

144 Kristine L. Gallardo, *Taming the Internet Pitchfork Mob: Online Public Shaming, the Viral Media Age, and the Communications Decency Act*, 19 VAND. J. ENT. & TECH. L. 721, 736 (2017).

145 *Id.* at 736–37. *See also* 47 U.S.C. § 230(f)(2) (defining "interactive computer service" as "any information service, system, or access software provider that

qualify as an ICS including classified ads websites, dating websites, and social media platforms.[146] Second, the ICS must be framed as the publisher or speaker of the content.[147] Third, the content must be created by another user, not the ICS.[148] This generally means that an ISP is not liable for third party tortious content unless the ISP elevates its involvement with the content; if it does, the ISP is no longer a passive "ICS" but instead an "information content provider" ("ICP").[149] If that shift in involvement occurs, the ISP will not qualify for immunity.[150] Unlike an ISP, an ICP is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other [ICS]."[151] There is an additional layer of protection aside from the framework because courts do not see ISPs as ICPs when "performing editorial functions, choosing to remove or add content, or making minor adjustments to third party content."[152]

Some courts have created additional standards for interpreting the CDA's immunity provision. For example, the Ninth Circuit created a test in *Barnes v. Yahoo! Inc.*[153] that joined together Subsection 230(e)(3) and 230(c)(1) and determined it only protects from liability: "(1) a provider or user of an [ICS] (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another ICP."[154]

Previously, the Ninth Circuit in *Fair Housing Council of San Fernando Valley v. Roommates.com*[155] had found that a:

provides or enables computer access . . . to the Internet and such systems operated or services offered by libraries or educational institutions.").

146 Gallardo, *supra* note 144, at 737.

147 Gallardo, *supra* note 144, at 737.

148 Gallardo, *supra* note 144, at 737.

149 Gallardo, *supra* note 144, at 737; *see also* Johnson, *supra* note 33, at 289 (finding immunity is not an absolute guarantee; if the intermediaries "materially contribute" to the creation of unlawful content on the platform it loses immunity).

150 Gallardo, *supra* note 144, at 737.

151 47 U.S.C. § 230(f)(3).

152 Gallardo, *supra* note 144, at 737.

153 Barnes v. Yahoo! Inc., 507 F.3d 1096 (9th Cir. 2009).

154 *Id.* at 1100–01.

155 Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157 (9th Cir. 2007).

> website operator can be both a service provider and a content provider: If it passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content. But as to content that it creates itself, or is "responsible, in whole or in part" for creating or developing, the website is also a content provider. Thus, a website may be immune from liability for some of the content it displays to the public but be subject to liability for other content.[156]

Utilizing that standard, the court determined immunity did not apply because *Roommates.com* acted as an ICP when it required website users to answer questions.[157] The court concluded that by requiring users to fill out questionnaires, the website contributed to the user-generated content.[158]

The bounds of the *Roommates* precedent remain unclear; it is likely that the CDA will continue to partially shield platforms from liability.[159] A platform could face liability for other actions such as putting branding on elicited content or creating an interface for conducting transactions.[160] After the *Roommates.com* decision, there were many contradictory judicial decisions as courts expressed doubts regarding the scope of immunity.[161]

The Ninth Circuit is one of the only courts that has taken action toward limiting CDA immunity for ISPs by excluding immunity to ISPs that "materially contribute" to the content or conduct in dispute.[162] Many courts instead align with the Sixth Circuit precedent that even if an ISP encourages or ratifies the content of a third party, it does not forfeit CDA immunity.[163] The

156 *Id.* at 1162–63.

157 Lobel, *supra* note 52, at 145–46.

158 Lobel, *supra* note 52, at 145–46.

159 Lobel, *supra* note 52, at 146.

160 Lobel, *supra* note 52, at 146.

161 Lavi, *supra* note 51, at 515.

162 Gallardo, *supra* note 144, at 738.

163 Gallardo, *supra* note 144, at 738. *See also* Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 417 (6th Cir. 2014).

Sixth Circuit is not alone in this determination as courts traditionally interpret the CDA's immunity provision broadly, repeatedly protecting online platforms from lawsuits.[164] Another example is *Reit v. Yelp, Inc.*[165] where a dentist sued Yelp for defamation and claimed that "Yelp should lose CDA immunity because its removal of positive posts was beyond the normal editorial function" protected.[166] The New York Supreme Court disagreed with the plaintiff, finding instead that the CDA barred the claim because a third party supplied the information on Yelp, and continued to say that Yelp's selection of the posts could be considered the selection of material for publication, an act which is a publisher's role.[167]

There has been a recent shift within the courts barring CDA immunity when public policy weighed against a finding of immunity or the defendant played a significant role in the content.[168] Despite this shift, as a general practice, courts continue to err on the side of granting immunity.[169] Unfortunately, even though courts' findings of immunity are consistent, the standards and practices they utilize to reach those findings are not uniform.[170] While the limits on the CDA are not clear, they are essential because immunity was not intended to create "a lawless no-man's-land on the Internet,"[171] but inconsistent court applications and interpretations of when an ISP becomes a content provider is starting to make immunity look lawless.

164 Lavi, *supra* note 51, at 513.

165 Reit v. Yelp, 907 N.Y.S.2d 411 (N.Y. App. Div. 2010).

166 *See Reit*, 907 N.Y.S.2d at 411; Andre Jaglom, *Internet Distribution, E-Commerce and other Computer Related Issues: Current Development in Liability Online, Business Methods Patents and Software Distribution, Licensing and Copyright Protection Questions*, ALI CLE Study Materials, 33 (June 2014).

167 Jaglom, *supra* note 166, at 33.

168 Jaglom, *supra* note 166, at 35.

169 Lavi, *supra* note 51, at 517.

170 Lavi, *supra* note 51, at 517.

171 Lavi, *supra* note 51, at 514.

IV. CRITICISMS AND CHALLENGES TO EFFECTIVE IMPLEMENTATION

In enacting SAVMA, the Australian government did not seek input from technology companies before passing the law, causing many to worry about the free speech impact, the burden on technology companies, and the overall effectiveness of the law.[172] This law has been critiqued by many experts in the field. Founder of the Dangerous Speech Project at Harvard's Berkman Klein Center for Internet Society, Susan Benesch, fears that this decision by Australia will lead to more dramatic responses from platforms such as increased censorship and takedowns and moving offices out of countries with these types of laws.[173] Another critique from Sunita Bose, Managing Director of Digital Industry Group Inc. ("DiGi"),[174] is that SAVMA does not address any of the hate speech that arose in the wake of the Christchurch Massacre.[175] Further, the legislation possesses multiple ambiguities, such as the meaning of the terms "expeditiously" and "in a reasonable time," raising questions about the effectiveness and potential legal impact and reach of the new law.[176]

The United Nations ("U.N.") Special Rapporteur on Counterterrorism and Human Rights and Freedom of Expression is an independent expert appointed by the United Nations Human Rights Council who is responsible for gathering, requesting, and exchanging information on alleged violations of human rights and fundamental freedoms while countering terrorism.[177] SAVMA's infringement upon the ability of individuals to share content in the name of protection from terrorism makes the opinion of the Special Rapporteur

---

172 Cave, *supra* note 6.

173 Cave, *supra* note 6.

174 A non-profit industry association advocating for digital rights within Australia with Google, Facebook, and Twitter as members. DIGI, https://digi.org.au/about/ (last visited Oct. 2, 2021).

175 Cave, *supra* note 6.

176 *See* Douek, *supra* note 40.

177 *Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER, https://www.ohchr.org/en/issues/terrorism/pages/srterrorismindex.aspx (last visited Oct. 2, 2021).

significant because it looks to discover issues with fundamental freedoms when preventing terrorism.[178] The U.N. Special Rapporteur critiqued the law, arguing ambiguities around "terrorist act" and "expeditiously" threaten freedom of expression because this lack of clarity encourages companies to take down material if it possibly qualifies as "abhorrent violent material."[179]

Critics predicted that the vague standards and high penalties articulated in SAVMA will cause service providers to take down more material in an abundance of caution, which will have a negative impact on the free speech and ideas expressed on the platform.[180] Further, it is challenging for Australia to enforce the removal and punish platform providers.[181] Despite the enforcement obstacle, the removal requirement created by the law applies to platforms, content services, and Internet service providers, many of whom lack the resources required to assess and remove content.[182]

Contrarily, the CDA gives platforms too much leeway to make decisions with no accountability system in place and no overarching guidelines. By prioritizing the protection of speech on social media platforms, the CDA gives platforms exclusive control over speech on the platform.[183] This allows a platform to choose either to not take down content, protect speech, and face accusations that the platform did not do enough to prevent harm or to remove harmful content and face accusations of censorship or failing to protect free speech.[184] Regardless of the choice selected, platforms avoid legal liability.[185] Effectively the CDA's Safe Harbor provision eliminated the "moderator's dilemma,"

178 *See* Douek, *supra* note 40.

179 Douek, *supra* note 40.

180 Douek, *supra* note 40.

181 Douek, *supra* note 40 (stating that Mark Zuckerberg Chairman, CEO, and controlling shareholder of Facebook refused to appear before an international committee of lawmakers for hearings in the U.K. concerning data privacy). *See also* Kelvin Chan, *Global Lawmakers Grill Facebook Exec; Zuckerberg's a No-show*, ASSOCIATED PRESS (Nov. 27, 2018), https://apnews.com/article/d471bb130d014556ac90aac3c42de1b9.

182 Douek, *supra* note 40.

183 Johnson, *supra* note 33, at 288.

184 Johnson, *supra* note 33, at 289.

185 Johnson, *supra* note 33, at 288.

that traditionally made platforms face the choice of not regulating content and maintaining its publisher status or regulating content, becoming a publisher, and facing liability for that content.[186] The Safe Harbor provision did this by offering the option to restrict access to information or to not take action and avoid liability either way.[187]

One particular area where the lack of accountability harms users is doxing. The CDA applies to doxing by creating a shield from liability for online service providers and thus removes a potential pathway to a doxing remedy.[188] Doxing, the malicious publication of personal information, is a form of online harassment that causes significant real-world harm.[189] Doxing does not necessarily require a hack to access the personal information, for example, a victim's home address or other information can be used to locate a subject.[190] In doxing, the aggressor moves the harassment from the Internet into the physical world by making personal information more accessible on the Internet, increasing the potential for harassment, injury, or violence.[191] Therefore, doxing has one foot online and one foot in the physical world, presenting a unique challenge. Further, victims cannot efficiently utilize the legal process because there is no consistent remedy for doxing.[192] This makes the CDA immunity for platforms even more troubling because victims of doxing cannot rely on the legal process to be made whole for the tortious conduct they experienced.

Ultimately, the CDA created overbroad protection for many companies while allowing individuals to post "without fear."[193] CDA immunity allows platforms to avoid content regulation and

186 David Opderbeck, *Judicial Activism Can't Fix Section 230*, BULWARK (Feb. 18, 2021, 5:47 AM), https://thebulwark.com/judicial-activism-cant-fix-section-230/.

187 *Id.*; *see also* 47 U.S.C.A § 230(c).

188 Julia M. MacAllister, *The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*, 85 FORDHAM L. REV. 2451, 2468 (2017). *See generally* Natalia Homchick, *Reaching Through the "Ghost Doxer:" An Argument for Imposing Secondary Liability on Online Intermediaries*, 76 WASH. & LEE L. REV. 1307, 1315 (2019).

189 MacAllister, *supra* note 188, at 2453.

190 MacAllister, *supra* note 188, at 2457.

191 MacAllister, *supra* note 188, at 2457.

192 MacAllister, *supra* note 188, at 2457.

193 Pagano, *supra* note 13, at 532–33.

liability, allowing the growth of a trillion-dollar industry for platforms that enable user-generated content sharing.[194] While many have been concerned about the potential impact for groups such as terrorists, human traffickers, or criminals using these platforms, political conservatives began advocating for more guidelines that prevent social media platforms from restricting posts online.[195]

The Trump Administration took umbrage with the CDA and even issued an executive order seeking to curtail the censorship of certain political ideas and ideologies.[196] Specifically, the order sought to prevent the social media platforms from handpicking content that should be excluded from the public discourse on their platforms and engaging in what the administration referred to as "selective censorship."[197] The order blames the CDA's immunity provision for the selective content removal and urges the Secretary of Commerce and Attorney General, acting through the National Telecommunications and Information Administration ("NTIA"), to redefine and limit the scope of the immunity.[198] Further, the order requested the NTIA file a petition for rulemaking with the Federal Communications Commission ("FCC") to clarify when an action is not "taken in good faith" and the circumstances under which a provider of an ICS cannot claim protection after restricting access to content inconsistent with the CDA.[199] But many experts found the order misinterpreted the CDA and would actually stifle speech even further because platforms would likely remove much of the questionable content to avoid liability for the content.[200]

---

194 Pagano, *supra* note 13, at 532.

195 Opderbeck, *supra* note 186.

196 Exec. Order No. 13925, 85 Fed. Reg. 34079 (June 2, 2020). *See also* Jeff Neuburger, *Commerce Dept. Petitions FCC to Issue Rules Clarifying CDA Section 230,* JD SUPRA (Aug. 3, 2020), https://www.jdsupra.com/legalnews/commerce-dept-petitions-fcc-to-issue-50397/.

197 Exec. Order No. 13925, 85 Fed. Reg. 34079 (June 2, 2020). *See also* Jeffrey Neuburger, *Commerce Dept. Petitions FCC to Issue Rules Clarifying CDA Section 230,* JD SUPRA (Aug. 3, 2020), https://www.jdsupra.com/legalnews/commerce-dept-petitions-fcc-to-issue-50397/.

198 Exec. Order No. 13925, 85 Fed. Reg. 34079 (June 2, 2020).

199 *Id.*

200 Anna Wiener, *Trump, Twitter, Facebook and the Future of Online Speech*, THE NEW YORKER (July 6, 2020), https://www.newyorker.com/news/letter-from-

Despite the miscalculation in the Executive Order, the Trump Administration did implement two laws that limited the immunity available under the CDA by holding websites that hosted sexual advertisements liable for that content. In 2018, Congress passed the House bill, FOSTA, and the Senate bill, SESTA, the Stop Enabling Sex Traffickers Act (collectively "FOSTA-SESTA"), which effectively curtailed the immunity provided by the Safe Harbor in the CDA.[201] These acts created an exception to the immunity provided to platforms under the CDA so that websites could be held accountable for ads for sex work.[202] This change was spurred by the use of Backpage, a website used for trafficking, because when victims filed lawsuits the website was able to hide behind the Safe Harbor provision of the CDA.[203] As a result, legislators introduced FOSTA-SESTA to narrow the immunity afforded to platforms by making websites "liable for any content that helped facilitate sex trafficking or prostitution" in all circumstances.[204]

While the goal of these laws was to monitor websites and provide the opportunity for sex trafficking survivors to sue their abusers, these laws had a significant negative impact on the consensual sex worker community.[205] The restrictions conflate consensual sex work with nonconsensual sex work and consequently prevent consensual sex workers from sharing information or warning each other about violent clients, thus

silicon-valley/trump-twitter-facebook-and-the-future-of-online-speech (pointing out that without CDA liability, content such as Trump's tweet suggesting MSNBC host Joe Scarborough murdered member of his staff would likely be removed).

201 Liz Tung, *FOSTA-SESTA was Supported to Thwart Sex Trafficking. Instead, it's Sparked a Movement*, WHYY (July 10, 2020), https://whyy.org/segments/fosta-sesta-was-supposed-to-thwart-sex-trafficking-instead-its-sparked-a-movement/. *See also* 18 U.S.C. § 1591 (2018); 18 U.S.C. § 2421A (2018).

202 *See* 47 U.S.C.A. § 230(e)(5); Aja Romano, *A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as We Know It*, VOX (July 2, 2018), https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-Internet-freedom; Glenn Kessler, *Has The Sex-trafficking Law Eliminated 90 Percent of Sex-trafficking Ads?*, WASH. POST (Aug 20, 2018), https://www.washingtonpost.com/politics/2018/08/20/has-sex-trafficking-law-eliminated-percent-sex-trafficking-ads/.

203 Tung, *supra* note 201.

204 Tung, *supra* note 201.

205 Romano, *supra* note 202.

making their work even more dangerous than before the new laws.[206] Further, there is limited evidence that FOSTA-SESTA reduced the amount of sex trafficking.[207] There is not a lot of research on the impact of the laws, but a new bill, SAFE SEX Workers Study Act, seeks to remedy that by ordering a study of the effectiveness of FOSTA-SESTA.[208] The government claimed the law did reduce sex trafficking ads by 90%, but by August 11, 2018, the advertising rebounded to almost 75% of the pre-FOSTA-SESTA rate.[209] The reverberating impact of limiting speech and harming consensual sex workers seemingly without achieving the goals indicates that making addenda to the CDA's immunity provisions is not enough to ensure platforms face liability.

Both SAVMA and the CDA highlight how legislatures are grappling with the evolution of social media platforms. While social media platforms started as neutral forums allowing users to post any content, the sites evolved and now platforms monitor and remove more messages, which requires the companies to rely on technology, such as artificial intelligence ("AI"), to help monitor content.[210] AI has enabled platforms to take down offensive content before it can even be flagged for some offensive content such as child-nudity posts; but other types of content are harder for AI to identify such as bullying or harassment posts which typically are only removed after they are reported by users.[211] Further, there are still millions of posts and profiles to sift through, which presents a challenge even for an AI tool.[212] For example, Twitter removed 2.9 million tweets over six months in 2019, YouTube removed 11.4 million videos in one quarter,

206 Romano, *supra* note 202; Karol Markowicz, *Congress' Awful Anti-sex-trafficking Law Has Only Put Sex Workers in Danger and Wasted Taxpayer Money*, BUSINESS INSIDER (July 14, 2019, 8:38 AM), https://www.businessinsider.com/fosta-sesta-anti-sex-trafficking-law-has-been-failure-opinion-2019-7.

207 Tung, *supra* note 201.

208 Tung, *supra* note 201; *see also* SAFE SEX Workers Study Act, H.R. 5448, 116th Cong. (2020).

209 Kessler, *supra* note 202.

210 *Social Media's Struggle with Self-censorship*, ECONOMIST (Oct. 22, 2020), https://www.economist.com/briefing/2020/10/22/social-medias-struggle-with-self-censorship.

211 *Id.*

212 *Id.*

and Facebook removes 17 million fake accounts each day.[213] This emphasizes that regulating platforms is a challenging task simply due to the vast amount of posts from users.

Both SAVMA and the CDA face criticism and have opportunities to improve. But the interesting dichotomy is that SAVMA is critiqued for not considering the needs of platforms and providers, while the CDA is critiqued for providing too much freedom to platforms. This suggests there is a middle ground available that the CDA should strive to meet with updates to the legislation.

V. DESIRED CDA CHANGES

The Trump Administration tried to claw back liability for censorship purposes but missed the point—the government should be clawing back liability for platforms more broadly. The issue of censorship is a concern for free speech, but the more pressing issue is that individuals damaged by third party posters should have a means to hold platforms and intermediaries accountable. There needs to be a balance, as an amendment to the CDA should not be a "kneejerk reaction" to the harms social media platforms facilitate against individuals and society.[214] Moreover, a codified consistent requirement within the CDA is essential so that users know what content is acceptable and platforms know they can be held accountable and how they can avoid liability.

The first option is to amend the CDA so that there is more accountability, obligations, and clarity around what the Good Samaritan provision requires of content providers. This choice supports the policy goals underlying the CDA.[215] Within the Good Samaritan provision, Congress endorsed an editorial role for Internet services, which have grown into today's social media platforms.[216] As the types of services provided by the Internet have evolved, so too should the CDA.[217] The varied responses by social media platforms to Trump after the attack on the Capitol

213 *Id.*

214 Johnson, *supra* note 33, at 309.

215 Bridy, *supra* note 14, at 219.

216 47 U.S.C.A. § 230(c); Bridy, *supra* note 14, at 219.

217 Bridy, *supra* note 14, at 219.

indicate that there is a greater need for consistency in acceptable content across platforms, as well as punishment by platforms against users. If there was a codified list of unacceptable content, such as the definition of "abhorrent violent material" within SAVMA, that could be a good starting point for the CDA to ensure consistency in content quality across platforms. [218]

Another approach would be to reconsider, reframe, and redraft how platforms should act in the context of the Good Samaritan provision.[219] Adding parameters around what actions must be taken under the Good Samaritan provision will allow for a more effective and consistent response to information problems such as hate speech, violent threats, harassment, doxing, and other online abuse.[220] This could be akin to SAVMA's provisions providing that content and hosting services must take content down or else they will be put on notice by a government group, which presumes that they were reckless and holds them accountable for their failure to take down harmful content.[221] By providing more clarity about processes and procedures for noncompliant material, the CDA can create guidelines for platforms and boundaries for users so that the online community can be a safer space.

To buttress those ideas, Congress should enact further additions to the CDA framework, including notice and takedown procedures for defamatory materials posted online, in a way that effectively balances the CDA's goals of promoting creative Internet growth and addressing the needs of online attack victims who are seeking content removal and compensation for tortious conduct.[222] This change requires platforms to "take down offensive content once . . . notified," and Congress could assign the FCC the role of creating "guidelines for companies to help determine which types of communications should be taken down" to ensure consistency.[223]

---

218 *Sharing of Abhorrent Violent Material Amendment Act 2019* (Cth) s 1 (Austl.).

219 *See* Bridy, *supra* note 14, at 219-20.

220 *See* Bridy, *supra* note 14, at 220.

221 *Sharing of Abhorrent Violent Material Amendment Act 2019* (Cth) s 1 (Austl.).

222 Gallardo, *supra* note 144, at 740.

223 MacAllister, *supra* note 188, at 2469.

While some social media companies have banned Trump as well as accounts and hashtags affiliated with voting conspiracies and the violence perpetrated in the wake of the election, independent action that is not codified by the CDA can lead to inconsistent approaches for preventing violent conduct.[224] The inconsistent approach is already evidenced by the platforms taking their action. For example, Twitter permanently banned Trump's account while YouTube implemented a strike system requiring users to get three strikes within ninety days to receive a permanent ban from the platform.[225] If there was a clearer policy about the type of content that would not be tolerated, like in SAVMA, and what obligations surrounded such content, there could be a consistent approach and a consistent ability to hold platforms accountable for failing to comply during violent outbreaks such as the attack on the Capitol.

Another suggestion is to amend the CDA to deny immunity to ISPs that make editorial and publication decisions on the theory that these entities are more than passive host sites for third party content.[226] By making editorial and publication decisions, the ISP engages in content creation and no longer just presents third party ideas.[227] This change would be in line with the Ninth Circuit precedent, but this alone is not sufficient to ensure that people have greater methods for restitution when they face online harassment.[228] It is a step in the right direction, but more is required to fully address the needed update to the CDA, such as clear procedures for taking down posts and guidelines for acceptable content.

Another option is to completely repeal the CDA and revert to the use of notice-based liability for third party tortious content, similar to the process utilized prior to the implementation of the

---

224 *See* Sara Fischer and Ashley Gold, *All The Platforms That Have Banned or Restricted Trump So Far*, AXIOS, (Jan. 11, 2020), https://www.axios.com/platforms-social-media-ban-restrict-trump-d9e44f3c-8366-4ba9-a8a1-7f3114f920f1.html.

225 Fischer *supra* note 224.

226 Gallardo, *supra* note 144, at 740.

227 Gallardo, *supra* note 144, at 740.

228 Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1176 (9th Cir. 2007) (holding that websites that not only passively display content but also create or partially create or develop content may not qualify for immunity).

CDA.[229] But this again would lead to inconsistent protection for individuals. Despite the challenges presented by inconsistent outcomes, a case-by-case basis could limit the benefits social media companies receive from hateful content today because each individual would have the unique circumstance of his case evaluated. Another potential drawback is that a lack of immunity protection could foster over-policing by social media platforms and other service providers for fear of liability, which could greatly limit free speech online.

VI. CONCLUSION

While the Internet today has greatly evolved from the Internet that existed when the CDA was first enacted, the CDA needs to face its own evolution. By codifying regulations that create consistent parameters across hosting and content service providers and explain (1) the type of content that must be removed; (2) the timeline for when it must happen; and (3) the repercussions for not complying, the CDA can take the guesswork and self-regulation away from technology companies. This change could provide consistent regulation for platforms and a clear pathway of relief for victims of online harassment and hate. SAVMA is a great example of defining content, creating parameters, and establishing repercussions, but the CDA can build upon that and provide greater clarity and detail to avoid the mistakes of ambiguity within SAVMA. The punitive response by social media companies to Trump's promotion of fake news about the election and the reverberating impacts indicate that now is a good time for all stakeholders to discuss a solution that is not only manageable for platforms but also sufficiently protects users. It is time that the protections promulgated on a case-by-case basis are codified to allow for consistent application of community norms and rules protecting both free speech and victims of online hate.

[229] Gallardo, *supra* note 144, at 740.