ARTICLE

FROM TERRORISTS TO TROLLS: EXPANDING WEB HOST LIABILITY FOR LIVE-STREAMING, SWATTING, AND CYBERBULLYING

ELIZABETH M. JAFFE[1]

CONTENTS

[1] Elizabeth M. Jaffe is an Associate Professor at Atlanta's John Marshall Law School. The author thanks her research assistant, Jordan Riser, for her invaluable assistance with the article.

INTRODUCTION

The New Zealand mosque attack, that took the lives of over fifty people and injured many more, evidences the desperate need to hold major web hosts such as Facebook and Twitter liable for perpetuating violence, terrorism, cyberbullying, and mass murders. While sites like Facebook and Twitter are common places where people from all over the world can connect, share opinions, watch the latest shows, and read the news, these sites have now become the main forum for cyberbullying, stalking, and harassment.[2] Although social media can bring a user closer to like-minded people, it also opens the door to hatred, abuse, and death threats.[3] Days before the New Zealand mosque attack, the alleged shooter, Brandon Tarrant, posted a 74-page white-nationalist manifesto on Twitter outlining his hatred and violence.[4] Then, on the day of the mosque attack, Tarrant strapped a camera to his helmet, while saying "Let's get this party started!" and streamed the attack on Facebook Live for the world to witness the atrocity.[5] Tarrant's use of Facebook Live and Twitter to spread his rage and broadcast a massacre reiterates the evolution of the 21st century type of harassment which has transformed online bullies and harassers into real-life trolls, terrorists, swatters, and murderers.[6]

As the use of social media and technology becomes more prevalent in our daily lives, the law must step in and hold web host giants liable. Social media users on Facebook and Twitter are allowed to echo their racism, sexism, homophobia, or religious extremism online, but there are few options for victims of this 21st century type of harassment.[7] We now live in the age where

---

[2] *See* Chris Wright, *In a World Consumed by Technology, We Must Have the Power to Switch Off*, HUFFINGTON POST (Mar. 28, 2018), https://www.huffingtonpost.co.uk/chris-wright1/in-a-world-consumed-by-te_b_15580306.html.

[3] *Id.*

[4] Shibani Mahtani, Wilma McKay & Kate Shuttleworth, '*Hiding in Plain 'Sight': In Quiet New Zealand City, Alleged Gunman Plotted Carnage*, WASH. POST (Mar. 21, 2019, 9:36 PM), https://www.washingtonpost.com/world/asia_pacific/hiding-in-plain-sight-in-quiet-new-zealand-city-alleged-gunman-plotted-carnage/2019/03/21/1846de9e-4a7b-11e9-8cfc-2c5d0999c21e_story.html [https://perma.cc/GN26-7V3B] (reporting that Tarrant trolled the darkest corners of the internet in hopes of finding inspiration and commonalities for his white-nationalist ideologies).

[5] Steven Hendrix & Michael E. Miller, *'Let's Get This Party Started': New Zealand Shooting Suspect Narrated His Chilling Rampage*, WASH. POST (Mar. 15, 2019), https://www.washingtonpost.com/local/lets-get-this-party-started-new-zealand-gunman-narrated-his-chilling-rampage/2019/03/15/fb3db352-4748-11e9-90f0-0ccfeec87a61_story.html [https://perma.cc/2YSF-9K62].

[6] Christopher Mims, *It's Hard to Spot the Terrorists Among the Trolls*, WALL ST. J. (Mar. 15, 2019, 5:33 PM), https://www.wsj.com/articles/its-hard-to-spot-the-terrorists-among-the-trolls-11552685615 [https://perma.cc/F95Q-7KUY].

[7] *See* Anti-Defamation League, *Quantifying Hate: A Year of Anti-Semitism on Twitter*, ADL.ORG (Apr. 16, 2019), https://www.adl.org/resources/reports/quantifying-hate-a-year-of-anti-semitism-on-twitter#introduction [https://perma.cc/B8E9-X3DX] (estimating that

cyberbullies are no longer creeping behind computer screens and clicking on keyboards.[8] Instead, they are using Facebook and Twitter to display and act on their rage with few consequences.[9] There needs to be a form of recourse for allowing web hosts who create and tolerate breeding grounds for mass shootings and murders and avoid liability for doing so.

This article explores the transformation of social media platforms such as Facebook and Twitter into arenas of cyberbullying, swatting, and even terrorism. Part I of this article focuses on the trend of technology advancement, the use of Facebook and Twitter, and its intersection with the law. Part II examines the current laws surrounding web host immunity and attempts to redefine web host immunity. Part III discusses possible methods for holding web hosts liable and highlights the critical need for legislation that will hold these social media platforms responsible for reasonably foreseeable harm.

I. MAKING IT A CRIME OVER TIME

In 2017, now-retired U.S. Supreme Court Justice Anthony Kennedy recognized just how far social media and the Internet consume our daily lives.[10] In *Packingham v. North Carolina*, Justice Kennedy noted: "While in the past there may have been difficulty in identifying the most important places . . . for the exchange of views, today the answer is clear. It is cyberspace . . . ."[11] If cyberspace is now one of the most important places for the exchange of views, similar to that of a public forum, then there need to be restrictions when people like Tarrant use these forums to showcase murder and other violent acts.

In 2008, North Carolina attempted to control such hate and abuse across the Internet when it enacted §14-202.5.[12] This statute made it a Class I felony for "a registered sex offender "to access a commercial social networking Web site where the sex offender knows that the site permits minor children to become members or to create or maintain personal Web pages."[13] Although the U.S. Supreme Court ultimately struck down the statute for being overbroad and not narrowly tailored to serve the State's legitimate interest, the *Packingham* court noted in its opinion that the "government, of course, need not simply stand by and allow these evils to occur" because the "sexual abuse of a child is a most

approximately 4.2 million anti-Semitic tweets were posted and reposted on Twitter between January 29, 2017 and January 28, 2018).

[8] *See* Mims, *supra* note 5.

[9] *Id.*

[10] David L. Hudson Jr., *Free Speech or Censorship? Social Media Litigation is a Hot Battleground*, A.B.A. J. (Apr. 1, 2019, 12:05 AM), http://www.abajournal.com/magazine/article/social-clashes-digital-free-speech [https://perma.cc/MC5T-NGVQ].

[11] Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017).

[12] *See id*. at 1733.

[13] *Id.* at 1731.

serious crime and an act repugnant to the moral instincts of a decent people."[14] If the government cannot "stand by" and let sexual abuse and harassment foster in cyberspace, social media giants like Facebook and Twitter must also be held responsible for broadcasting a massacre of a targeted group of people on its website. Justice Kennedy's discussion in *Packingham* and North Carolina's attempted legislation show that both the Supreme Court and the States are trying to adapt to the use and exploitation of social media platforms and determine how these platforms intersect with the law.

Moreover, Justice Kennedy's discussion in *Packingham* highlights one crucial part of the evolution of technology and social media.[15] The events that took place in New Zealand, including Tarrant's use of Facebook to broadcast such crimes, create the need for methods to hold web hosts liable. Author David Hudson notes that while social media companies like Facebook and Twitter are not subject to First Amendment constraints, the rise of expression that entices hate and calls for violence, rages across these platforms and these platforms may become obligated to regulate private expressions.[16] With the evolution of Facebook and Twitter, hate and violence are now unavoidable on the Internet.[17] Fifty-three percent of Americans say they experienced hateful speech and harassment in 2018, and thirty-seven percent reported severe attacks, including sexual harassment and stalking.[18] One-third of Americans experienced online abuse in response to their sexual orientation, religion, race, ethnicity, gender identity or disability.[19]

Online threats are turning into real-world acts of violence and terror.[20] In 2016, Facebook's live video' streaming feature became publicly available.[21] Any user with a Facebook account can log in and simply select the "Live Video" option from the dropdown menu.[22] Facebook Live enables the user to post and stream live video footage, and anyone can watch if the user selected the audience as public.[23] After Facebook began offering the live-streaming option, there have

[14] *Id.* at 1376.

[15] *See id.* at 1375.

[16] Hudson, *supra* note 9.

[17] *See* Jessica Guynn, *If You've Been Harassed Online, You're Not Alone. More than Half of Americans Say They've Experienced Hate*, USA TODAY (Feb. 13, 2019), https://www.usatoday.com/story/news/2019/02/13/study-most-americans-have-been-targeted-hateful-speech-online/2846987002 [https://perma.cc/8WBN-H2WH].

[18] *Id*.

[19] *Id*.

[20] *Id*.

[21] Paul Harper & Gemma Mullin, *Death on Camera: How Facebook Live Murder and Suicide Videos are Spreading Online and What You Should Do if You Spot Inappropriate Content*, THE SUN (Feb. 28, 2019), https://www.thesun.co.uk/news/3426352/facebook-live-clips-murder-suicide-shootings-report [https://perma.cc/34GA-4VMC].

[22] *Id.*

[23] *Id*.

been countless murders and acts of violence streamed across the platform.[24] In response, Facebook claims to have hired over three thousand employees to police hate-filled content.[25] Additionally, Facebook CEO, Mark Zuckerberg, wrote on his own Facebook page that he wanted to respond to reports of violence quickly.[26] But is a single statement promising to address the violence enough?

During the New Zealand attack, Tarrant's live video streamed for at least 17 minutes on Facebook Live before New Zealand Police notified Facebook about the video.[27] Facebook removed the video after being notified, but users reported the video was still widely available for hours after being first uploaded to Tarrant's Facebook account.[28] Facebook claims it removed the video immediately, suspended Tarrant's account, and also removed any praise or support for the crime or the shooter.[29]

Facebook claimed it would be working to combat this type of content, and it would be working directly with the New Zealand Police as their investigation continued.[30] Yet despite Facebook's attempt to regulate hate-filled content and violence, hiring thousands of content moderators and investing in artificial intelligence for content moderation, it has not been widely successful.[31] Author Donie O'Sullivan questions: "If the artificial intelligence systems built by one of the richest companies in the world can't identify and take action on a video containing weaponry, repeated gunfire and murder, what can they identify?"[32]

Facebook's chief technology officer, Mike Schroepfer, explained that Facebook's artificial intelligence systems could identify, with about ninety percent accuracy, the difference between pictures of broccoli and pictures of marijuana.[33] While this illustration is useful in understanding how Facebook's

---

[24] *Id*. (highlighting some of the tragic cases that were broadcasted on Facebook Live: Wuttisan Wongtalay hanged his eleventh-month-old daughter on Facebook Live; Ralph Hishaw broadcasted his six-year-old child being tortured on Facebook Live; Katlyn Nicole Davis filmed her suicide on Facebook Live; teen school girls bullied and brutally beat another classmate on Facebook Live; Jared McClemore died after he attempted to set fire to his girlfriend on Facebook Live; a fifteen-year-old schoolgirl was gang raped on Facebook Live).

[25] *Id*.

[26] *Id*.

[27] Donie O'Sullivan, *Facebook Says It's Policing Its Platform but It 'Didn't Catch a Livestream of a Massacre. Why?*, CNN BUS. (Mar. 15, 2019, 2:21 PM), https://www.cnn.com/2019/03/15/tech/facebook-new-zealand-content-moderation/index.html **[**https://perma.cc/F3JK-UC55].

[28] Reed Stevenson & Michael Tighe, *Facebook, YouTube Blindsided by Mosque Shooter's Live Video*, BLOOMBERG (Mar. 15, 2019), https://www.bloomberg.com/news/articles/2019-03-15/facebook-youtube-blind-sided-by-mosque-shooter-s-live-video [https://perma.cc/4XFW-SCTU].

[29] *Id.*

[30] *Id.*

[31] O'Sullivan, *supra* note 26.

[32] *Id.*

[33] *Id*.

artificial intelligence can fight against attempted drug sales online, being wrong ten percent of the time is not good enough.[34] If Facebook's artificial intelligence is failing to identify the difference between broccoli and marijuana ten percent of the time, imagine how many times it is failing to identify cyberbullying, violence, and graphic content.[35] The New Zealand tragedy is a frightening example of how Facebook and Twitter were ill-equipped to prevent such an atrocity. Although the web hosts are repeatedly claiming they are actively monitoring and quickly attempting to address these frightening situations, courts and state legislatures are realizing the necessity of minimizing hate-filled online content.[36] North Carolina's attempt to criminalize violence and abuse on social media is just one example of how States are seeking to monitor the situation and ultimately hold users of social media liable for their actions.[37]

A. Evolution of Technology: Extending Third Party Liability through Kubert v. Best

In 2013, a New Jersey Superior Court responded to the distracted driving epidemic that has plagued the nation,[38] by holding that a third party, who is texting from a remote location from the driver of a motor vehicle, can be liable to persons injured because the driver was distracted by the text.[39] The *Kubert* court extended liability if the third party texter knew or had special reason to know that the recipient will view the text while driving and an accident was caused by such texting.[40] While holding a third party texter liable provides compensation for the victims, the *Kubert* decision spoke to greater lengths.[41] By holding that a third party can be held responsible for sending a text to someone who is driving, the *Kubert* court highlighted the incentive to prevent the occurrence of harm all together by creating civil liability for such conduct.[42] The *Kubert* court used its authority and took direct, affirmative action to fight against the harm caused by distracted driving and to promote public awareness of the gravity of the harm.[43] If the *Kubert* rule is applied to the New Zealand mosque attack, Facebook and Twitter should be liable for knowing, or having reason to know, Tarrant could act on his white nationalist threats because he posted statements of his intent to commit violence on Facebook and Twitter just days

[34] *Id*.

[35] *Id*.

[36] *See id*.; *see also* Packingham v. North Carolina, 137 S. Ct. 1730, 1731 (2017).

[37] *See Packingham*, 137 S. Ct. at 1731.

[38] Morgan Gough, Comment, *Comments: Judicial Messaging: Remote Texter Liability as Public Education*, 44 U. BALT. L. REV. 469, 469 (2015).

[39] *Id.* (quoting Kubert v. Best, 75 A.3d 1214, 1218-19 (N.J. Super. Ct. App. Div. 2013)).

[40] *Id*. (citing *Kubert*, 75 A.3d at 1219).

[41] *Id*. at 470.

[42] *Id.* (quoting W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS 25 (5th ed. 1984)).

[43] *Id*. at 474.

before the attack.[44] The *Kubert* court proactively expanded liability and served to educate the public about the potential harm from the growing speed of technological advances.[45] While the *Kubert* court focused on a narrow class of technology users, the *Kubert* logic should be extended to web hosts that permit users to commit acts of violence and hate against others.[46]

B. Extending Third Party Liability by Criminalizing "Swatting"

As the *Kubert* court addressed the harm caused by a third party sending a text message to a remote driver, other forms of technology and cyberbullying are prevailing through the use of technology and the Internet. Now, cyberbullies can harass potential victims through a form of harassment called "swatting"—making a hoax call to 9-1-1 to draw a response from law enforcement, usually a SWAT Team.[47] The individuals who engage in swatting use technology to make it seem that the emergency call is coming from the victim's phone and convince 9-1-1 operators they are telling the truth.[48] When the SWAT team arrives at the victim's location, the victim is scared, taken by surprise, and in some situations, the results can be deadly.[49]

In the case of Andrew Finch, swatter Tyler Barriss "contacted Wichita authorities and reported that after a fight between his parents, he had shot and killed his father, held his mother and brother at gunpoint and threatened to light the house on fire before committing suicide."[50] After law enforcement responded to this false report, erroneously thinking Barriss was at a different address, a Wichita police officer fatally shot Andrew Finch.[51] While Barriss was sentenced to prison for making a hoax call that led to the tragic death of Andrew

[44] *See* Mahtani et al., *supra* note 3.

[45] *Id.* at 478.

[46] *Id.* at 485.

[47] *See The Crime of 'Swatting': Fake 9-1-1 Calls Have Real Consequences*, FBI (Sept. 3, 2013), https://www.fbi.gov/news/stories/the-crime-of-swatting-fake-9-1-1-calls-have-real-consequences1 [https://perma.cc/C3LK-W2M7].

[48] *Id.*

[49] *Id.*

[50] *See* Suzannah Gonzales, *California Man, Two Others Indicted in Fatal Kansas 'Swatting' Case*, REUTERS (May 23, 2018, 9:28 PM), https://www.reuters.com/article/us-kansas-swatting/california-man-two-others-indicted-in-fatal-kansas-swatting-case-idUSKCN1IP065 [https://perma.cc/EPY3-XC33] (reporting that "Barriss was charged with conveying false information and hoaxes, cyberstalking, threatening to kill another or damage property by fire, and transmitting interstate threats" and previously charged with involuntary manslaughter and interference with law enforcement).

[51] *Id.*; *see also* Matt Stevens & Andrew R. Chow, *Man Pleads Guilty to 'Swatting' Hoax That Resulted in Fatal Shooting*, N.Y. TIMES (Nov. 13, 2018), https://www.nytimes.com/2018/11/13/us/barriss-swatting-wichita.html [https://perma.cc/8YVD-BCSA] (reporting that Barriss pled guilty to making dozens of hoax phone calls during which he reported fake crimes, and will serve 20-25 years in prison).

Finch, in many situations authorities do not catch or prosecute the perpetrator.[52] However, individual States and Congress have started to address the epidemic by attempting to enact numerous laws combatting swatting and other forms of cyberbullying.[53]

In 2015, Senator Charles Schumer introduced to the Senate the SWAT Act, which provides that for any "false, fictitious, or fraudulent statement . . . to a Federal law enforcement agency that causes an emergency Federal law enforcement response, the term of imprisonment shall be not more than 8 years."[54] In addition, Congresswoman Katherine Clark introduced the Interstate Swatting Hoax Act, which would make it a crime for a person "with the intent to cause an emergency response by any law enforcement agency . . . [to] use[] a telecommunications system, the mails, or any other facility of interstate or foreign commerce to knowingly transmit false or misleading information . . . ."[55]

States including New Jersey, California, and Michigan have also addressed the necessity for enacting laws related to swatting. New Jersey Assemblyman Paul D. Moriarty proposed an Act (A3877) to upgrade the crime of false public alarm whenever it involves a false report or warning of an impending bombing, hostage situation, or person armed with a deadly weapon, to be punishable by up to ten years in prison, a fine up to $150,000, or both.[56] California also passed legislation in an effort to address swatting and false police reports by making it a crime "punishable by imprisonment in a county jail for a period not exceeding one year, or by a fine not exceeding one thousand dollars ($1,000), or by both that imprisonment and fine."[57] In Michigan, punishment for swatting can result in a maximum of ninety-three days of imprisonment in cases of misdemeanors, five years imprisonment and a twenty-five thousand dollar fine, in cases where a victim is injured, and no more than fifteen years in prison and a fine between twenty-five thousand dollars and fifty thousand dollars, if a death occurs as a result of the swatting.[58] While state and local legislatures are making some progress in confronting the harms resulting from the evolution of technology and social media, the question still remains: Why are the Web hosts still not liable?

---

[52] *See* John Keilman, *'Swatting' No Prank to Video Game Celebrities*, CHI. TRIB. (Sept. 12, 2014, 5:15 PM), https://www.chicagotribune.com/suburbs/bolingbrook-plainfield/ct-swatting-video-games-met-20140912-story.html [https://perma.cc/QX3G-HJZZ].

[53] *See, e.g.*, *infra* notes 54-58.

[54] Swatting Won't be Accepted or Tolerated Act of 2015, S. 1018, 114th Cong. § 1 (2015).

[55] Interstate Swatting Hoax Act, H.R. 4057, 114th Cong. § 2 (2015) (stating that if an emergency response results, the swatter will be fined, imprisoned up to five years, or both, that if serious bodily injury results, the swatter will be fined, imprisoned up to twenty years, or both, and that if the swatting results in death, the swatter will be fined, imprisoned for up to life, or both).

[56] Assemb. 3877, 216th Leg., Reg. Sess. (N.J. 2014).

[57] CAL. PENAL CODE § 148.3 (West 2016).

[58] MICH. COMP. LAWS ANN. § 750.411a(1) (West 2016).

II. ARE WEB HOSTS REALLY IMMUNE FROM LIABILITY?

A. The Trend Away from CDA Immunity

By enacting the Communication Decency Act ("CDA"), Congress acknowledged that the Internet and other interactive computer services offer a diverse forum for "political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[59] With growing use of the Internet, more Americans are relying on interactive media for an array of political, educational, cultural, and entertainment services, which have flourished with a "minimum of government regulation."[60] The CDA provides immunity from civil liability for providers or users of interactive computer services.[61] In enacting the CDA, Congress intended:

> (1) to promote the continued development of the Internet . . . (2) to preserve the vibrant and competitive free market that presently exists for the Internet . . . (3) to encourage the development of technologies which maximize user control over what information is received . . . (4) to remove disincentives for the development and utilization of blocking and filtering technologies . . . and (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.[62]

Essentially, the CDA precludes courts from placing a computer service provider in a publisher's role, even if the publisher is actively exercising its discretion in deciding whether to "publish, withdraw, postpone or alter content."[63] In *Zeran v. America Online, Inc.*, the Fourth Circuit noted that "the amount of information communicated via interactive computer services is . . . staggering."[64] The court further recognized that it would be "impossible for service providers to screen each of their millions of postings for possible problems."[65] However, as the use of technology rises and the use of artificial intelligence continues, the *Zeran* court's reasoning becomes flawed. Forty-nine percent of the world's largest tech companies are in the United States.[66] Of that

---

[59] 47 U.S.C. § 230(a)(3) (2012).

[60] *Id.* §§ 230(a)(4), (a)(5).

[61] *Id.* § 230(c).

[62] *Id.* § 230(b).

[63] Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

[64] *Id.* at 331.

[65] *Id*.

[66] Kristin Stoller, *The World's Largest Tech Companies 2017: Apple and Samsung Lead, Facebook Rises*, FORBES (May 24, 2017, 7:00 AM), https://www.forbes.com/sites/kristinstoller/2017/05/24/the-worlds-largest-tech-companies-2017-apple-and-samsung-lead-facebook-rises/#abc5545d140d [https://perma.cc/VRY3-6GV3].

forty-nine percent, eight of the top ten companies include Apple, Microsoft, Alphabet, IBM, Intel, Cisco Systems, Oracle, and Facebook.[67]

As these large tech companies become more technologically savvy, the artificial intelligence market extends its cognitive software capabilities.[68] Facebook uses algorithms powered by artificial intelligence to detect inappropriate content.[69] Recent reports indicate that global spending on artificial intelligence systems is projected to reach $77.6 billion in 2022, which is more than triple the $24 billion forecast for 2018.[70] Facebook's chief artificial intelligence officer, Yann LeCun, stated in a recent interview that the advancement of artificial intelligence technologies will include teaching machines to "learn about how the world works through data rather than learning how to solve one particular problem."[71]

LeCun noted that by training algorithms to identify data, Facebook will be able to improve real-time content moderation on its platforms instead of fixing the problems after the fact.[72] Though advances in technology and cybersecurity are incredibly expensive, Facebook's 2018 fourth-quarter revenue jumped to $16.9 billion, and profits rose to $6.9 billion.[73] Thus, it is not financially impossible for Facebook to screen for possible problems as the *Zeran* court once suggested.[74] As a result, the *Zeran* court's initial logic in granting immunity to web hosts like Facebook and Twitter is now contrary to the rise of artificial intelligence; consequently, recognizing the *Zeran* court's purpose for allowing web hosts to claim immunity is skewed in the new age of technology. Congress' initial intent behind enacting the CDA is also lost among the use of artificial intelligence.[75] The CDA can no longer stand as a barrier from liability for web

---

[67] *Id.*

[68] *See* Lisa Eadicicco, *3 Things We Learned from Facebook's AI Chief About the Future of Artificial Intelligence*, BUS. INSIDER (Feb. 18, 2019, 12:30 PM), https://www.businessinsider.com/facebook-artificial-intelligence-yann-lecun-2019-2 [https://perma.cc/6FD3-59ZB].

[69] *Id*.; *see also* Bernard Marr, *The Key Definitions of Artificial Intelligence (AI) That Explain Its Importance*, FORBES (Feb. 14, 2018), https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/#496e0aa94f5d [https://perma.cc/Z6LL-7CSR] (defining artificial intelligence as a sub-field of computer science and how machines can imitate human intelligence in the forms of visual perception, speech recognition, decision-making, and translation between languages).

[70] Eadicicco, *supra* note 67.

[71] *Id.* ("Such an advancement could be critical for Facebook as it ramps up its efforts to detect online bullying and identify content related to terrorism on its platforms.").

[72] *Id.*

[73] Mike Isaac, *Facebook's Profits and Revenue Climb as It Gains More Users*, N.Y. TIMES (Jan. 30, 2019), https://www.nytimes.com/2019/01/30/technology/facebook-earnings-revenue-profit.html [https://perma.cc/GFR6-QNP2].

[74] Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

[75] *See* 47 U.S.C. § 230(b) (2012).

hosts like Facebook and Twitter who fail to take action against cyberbullies, harassers, and users who hide behind hate-filled content.

Other courts also stray from the impossibility ideology standard stated in *Zeran*.[76] In *Jones v. Dirty World Entertainment,* the district court concluded a service provider will be held responsible for the development of offensive conduct if the site specifically encourages the development of what is offensive about the content.[77] In *Fair Housing Council of San Fernando Valley v. Roommates.com*, the court held that immunity would not be granted to service providers who actively become content providers themselves, in contrast to service providers who passively publish content or simply relay information from a third party.[78] Accordingly, the court in *Federal Trade Commission v. Accusearch* echoed the *Roommates* court's language by holding that a service provider becomes a content provider, and is thus not protected by the CDA if the web host is responsible as the cause of the injurious content.[79] Although there are numerous interpretations across the circuits as to when immunity may not be imputed, the CDA still allows web hosts to avoid liability after being notified of injurious content.[80]

B. Liability Through Common-Law Tort Theories

With the recent trend among courts recognizing a reduction in the CDA's power, it may become necessary to view web host liability through the concept of general common-law tort liability. In tort law, an actor has no duty to aid or protect a third party from harm even if the actor realizes or should realize that action on his party is necessary.[81] However, the exception to this general rule is where a special relationship exists,[82] or where an actor undertakes a duty to control the conduct of a third person as to prevent him from causing physical harm to another.[83] Other duties may be imposed on an actor if prior conduct is

[76] *See* Jones v. Dirty World Entm't Recording, 840 F. Supp. 2d 1008, 1012 (E.D. Ky. 2012).

[77] *Id.* at 1011. *But see* Jones v. Dirty World Entm't Recordings, 755 F.3d 398, 408, 415 (6th Cir. 2014) (vacating district court's ruling because defendants did not materially contribute to the defamatory content of statements but maintaining that CDA immunity is not without limits).

[78] Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157, 1166-67 (9th Cir. 2008).

[79] Fed. Trade Comm'n v. Accusearch, 570 F.3d 1187, 1198-99 (10th Cir. 2009).

[80] *See* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1103 (9th Cir. 2009).

[81] RESTATEMENT (SECOND) OF TORTS § 314 (AM. LAW INST. 1965).

[82] *Id.* § 314(a) (indicating the recognized special relationships are common carrier-passenger, innkeeper-guest, possessor of land-invitee, employer-employee, or one who is required by law or voluntary takes custody of another such as to deprive the other of his normal opportunities for protection; however, see comment (b) that indicates that this list is not intended to be exclusive).

[83] *Id.* § 321.

found to be dangerous,[84] if the actor knows he has caused such bodily harm,[85] or if the actor renders services to another which he should recognize as necessary for the protection of a third person.[86] According to Facebook's Terms of Service,[87] Mission Statement,[88] and previous attempts to monitor user content,[89] Facebook can hardly claim that it does not owe a duty to its users and can hardly rebut the fact that by undertaking such duty, that they can escape liability for the harm that they let happen.

C. Facebook Has a Duty

Facebook's own Community Standards page outlines what is and what is not allowed on Facebook.[90] Facebook alleges that the goal of the Community Standards is to "encourage expression and create a safe environment."[91] Under Facebook's Community Standards section, the web host claims that safety is one of its core values, and in service of that, Facebook might remove content that encourages real-world harm, including but not limited to physical, financial, and emotional injury.[92]

Facebook's stated mission is: "give people the power to build community and bring the world closer together."[93] Facebook further explains:

> Building community and bringing the world closer together depends on people's ability to share diverse views, experiences, ideas and information. We want people to be able to talk openly about the issues that matter to them, even if some may disagree or find them objectionable. In some cases,

[84] *Id.* (stating that there will be a duty imposed on the actor if such actor does an act, and subsequently realizes or should realize that it has created an unreasonable risk of causing physical harm to another and that this rule will apply even if the actor, at the time of the act, has no reason to believe that it will involve such a risk).

[85] *Id.* § 322 (noting that the duty to exercise reasonable care to prevent such further harm will remain whether the actor's conduct was tortious or innocent).

[86] *Id.* § 323 (reasoning that the actor is subject to liability if his failure to exercise such care increases the risk of harm or the harm is suffered because of the other's reliance upon the undertaking).

[87] *Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php [perma.cc/FP3T-CPYW].

[88] *About*, FACEBOOK, https://www.facebook.com/pg/facebook/about/ [perma.cc/ULC5-WFB8] ("Give people the power to build community and bring the world closer together.").

[89] *See* Eadicicco, *supra* note 67.

[90] *Community Standards*, FACEBOOK, https://www.facebook.com/communitystandards [https://perma.cc/9M76-HXQU].

[91] *Help Center: I don't think Facebook should have taken down my post*, FACEBOOK, https://www.facebook.com/help/2090856331203011 [https://perma.cc/QV9Z-VQ6S].

[92] *Community Standards: Safety*, FACEBOOK, https://www.facebook.com/communitystandards/safety [https://perma.cc/WDJ7-6ASG].

[93] Mark Zuckerberg, *Bringing the World Closer Together*, FACEBOOK (June 22, 2017), https://www.facebook.com/notes/mark-zuckerberg/bringing-the-world-closer-together/10154944663901634/ [https://perma.cc/WL49-WQQ4].

> we allow content which would otherwise go against our Community Standards – if it is newsworthy and in the public interest. We do this only after weighing the public interest value against the risk of harm and we look to international human rights standards to make these judgments.[94]

In accordance with its mission, Facebook's Community Standards purport to ensure an environment of safety.[95] Yet Facebook fails to take a strong stance against fighting against hate-filled content that cultivates into real-life violence. Facebook says it is committed to making the site a safe place,[96] so why are we not holding them liable when they fail to provide a safe environment for their users? With this undertaking to ensure a safe environment for users, tragic cases of harassment and death multiply across Facebook and make these claims far-fetched from Facebook's initial mission of ensuring a safe place for its users.[97] With growing numbers of harassment and cyberbullying, Facebook can hardly rebut that allowing this type of known conduct to continue without more intervention creates a toxic and dangerous forum for its users.

Facebook's Community Standards section also includes a subsection that provides the alleged actions Facebook takes against violence and criminal behavior.[98] Facebook, once again, alleges that it aims to "prevent potential offline harm that may be related to content on Facebook."[99] The web host claims that in order to prevent this type of offline harm, it takes the affirmative steps of removing language that incites or facilitates serious violence, removing content, disabling accounts, and working with law enforcement when it believes there is a "genuine risk of physical harm or direct threats to public safety."[100]

Further, in a stated effort to prevent and disrupt real-world harm, Facebook does not allow any organizations or individuals that proclaims a violent mission or engage in violence to have a presence on Facebook.[101] In the wake of the New Zealand massacre, the question remains: Why does a 74-page manifesto written on Tarrant's personal page, monitored by a web host, explicitly outlining his

---

[94] *Community Standards*, *supra* note 89.

[95] *Id.*

[96] *Id.*

[97] *See* Harper & Mullin, *supra* note 20.

[98] *Community Standards: Violence and Criminal Behavior*, FACEBOOK, https://www.facebook.com/communitystandards/violence_criminal_behavior [https://perma.cc/CFN9-Q8F3].

[99] *Id.* § 1.

[100] *Id.* (stating that Facebook also tries to "consider the language and context in order to distinguish causal statements from content that constitutes a credible threat to public or personal safety. In determining whether a threat is credible, [Facebook] may also consider additional information like a person's public visibility and vulnerability"").

[101] *Id.* § 2 (outlining the types of organizations as terrorist activity, organized hates, mass or serial murder, human trafficking, organized violence or criminal activity and also removing content "that expresses support or praise for groups, leaders, or individuals involved in these activities").

intent to commit real-world violence against a selected group of people not trigger any response for the web host to act to protect the people Tarrant targeted?[102] Facebook promises to take action to remove violence and crime, yet Facebook did not respond until the Facebook Live video was reported 29 minutes after the video started, 12 minutes after the live broadcast ended.[103] Perhaps the answer is simple; Facebook will not perform the duty it undertakes through its Community Standards because it knows that it will not face liability under the current laws. While Facebook may be pressured to enhance its security and prevent tragedies from happening,[104] the current laws do not impose liability on social media web hosts.[105]

III. POSSIBLE METHODS OF WEB HOST LIABILITY

The First Amendment protects hate speech unless it crosses the line into the unprotected categories of true threats, incitement to imminent lawless action, or fighting words.[106] Very few laws governing hate speech exist, but regardless of those laws, we are relying heavily on private web host companies to implement and uphold their terms-of-service agreements to fight against hate speech.[107] Based on this reliance, the websites are unfiltered and unrestricted in allowing for the internet to be the main recruiting ground for today's violence and hate-based groups.[108] Web hosts need to take further steps in regulating hate speech on their platforms.[109] University of Detroit Mercy Law Professor, Kyle

[102] *See* Mahtani et al., *supra* note 3.

[103] Chris Sonderby, *Update on New Zealand*, FACEBOOK NEWSROOM (Mar. 18, 2019), https://newsroom.fb.com/news/2019/03/update-on-new-zealand/ [https://perma.cc/9TBF-XFSM].

[104] *See* Makena Kelly, *Facebook, YouTube, and Others Asked to Brief Congress on New Zealand Shooting Response*, THE VERGE (Mar. 19, 2019, 4:57 PM), https://www.theverge.com/2019/3/19/
18273257/facebook-youtube-microsoft-twitter-congress-zealand-shooting-response
[https://perma.cc/LBJ2-PSH3] (Chairman of the House Homeland Security Committee, Representative Bennie G. Thompson, wrote to tech executives and CEOS of Facebook, YouTube, Twitter, and Microsoft urging them to prioritize the removal of terrorist content and to brief the committee on their response and plans for prevention).

[105] 47 U.S.C. § 230(c)(1) (2012); *see also* German Lopez, *It Took One Mass Shooting for New Zealand to Ban Assault Weapons*, VOX (Mar. 21, 2019, 11:20 AM), https://www.vox.com/2019/3/21/18272741/new-zealand-assault-weapons-ban-us-gun-laws [https://perma.cc/Z8RM-PC2D] (highlighting New Zealand's urgent response to the mosque attack, when Prime Minister Jacinda Ardern vowed that New Zealand gun laws will change, 24 hours after the attack. Less than a week later, Arden announced sweeping legislation that will be in full effect by mid-April).

[106] *See* Hudson, *supra* note 9.

[107] *Id.* (quoting Shannon Martinez, program manager for Free Radicals Project).

[108] *Id.*

[109] *Id.* (quoting Clay Calvert, director of the Marion B. Brechner First Amendment Project at the University of Florida College of Journalism and Communications).

Langvardt, suggests Congress should step in and create an administrative system that would handle online censorship issues, complaints, and oversights of their censorship practices.[110]

While web hosts like Facebook and Twitter should take more definite action to monitor and police hate-filled content, any restrictions on freedom of expression or speech raise a multitude of legal questions.[111] Since Congress has expressed little intent to amend the CDA or enact any other law to hold these web hosts liable,[112] another option is to focus on self-regulation for social media.[113] A self-regulation model would allow a board to employ a "national or regional press council, complaints commission, or ombudsperson."[114] These press councils would "publish their codes of conduct with the approval of journalistic and media organisations" and "accept complaints from any member of the public who believes that a published article [or post] infringes the respective code of conduct."[115] The members of the press council would then adjudicate the complaints, publish their findings, impose a right of reply on the offending outlet, and/or impose financial penalties on the web host.[116]

While there are possible problems with self-regulation models,[117] the benefits include independence from government, commercial, and special interests; and an open, transparent process allowing broad public consultation. A code of ethics for web hosts could be developed with a clear procedural system to determine if ethical standards are breached.[118] Essentially, a self-regulating press council or commission would take the duty of enforcing liability against web hosts out of the realms of the CDA and provide a viable solution to CDA immunity. Consequently, with adequate pressure from the government,[119] self-regulation is a plausible solution for holding web hosts liable.[120]

---

[110] *Id.*

[111] *See* ARTICLE 19, SELF-REGULATION AND 'HATE SPEECH' ON SOCIAL MEDIA PLATFORMS 4 (2018), https://www.article19.org/wp-content/uploads/2018/03/Self-regulation-and-%E2%80%98hate-speech%E2%80%99-on-social-media-platforms_March2018.pdf [https://perma.cc/GU73-RMWR].

[112] *But see* H.R. 11865, 115th Cong. (2018) (amending the Communications Act of 1934 to clarify that section 230 of the Act does not prohibit enforcement of criminal and civil law relating to sexual exploitation of children or sex trafficking against providers and users of interactive computer services).

[113] ARTICLE 19, *supra* note 110.

[114] *Id.* at 10.

[115] *Id.*

[116] *Id.*

[117] *Id.* at 11 (stating that often times self-regulatory bodies have been described as "elitist circle of enforcers" and sometimes have difficulty gaining public trust).

[118] *Id.* at 11-12.

[119] *Id.*

[120] *See id.* at 4-5.

IV. CONCLUSION

As the rise of technology and social media continues at a rapid rate, it is time for the law to place responsibility on web hosts who perpetuate a breeding ground for hate-filled content and expression that places others in harm. The New Zealand mosque attack was just one instance where content posted on social media turned deadly.[121] Web hosts like Facebook and Twitter have a duty to protect and monitor content to ensure that users do not turn hateful rhetoric into hateful real-life conduct. Without new methods to hold web hosts liable, cyberbullying will continue to occur not just in the dark corners of the web, but live-streamed for the world to view. Web hosts like Facebook and Twitter can no longer stand behind the principle of maintaining the public interest in user content when violent content directly turns into real-life tragedies.[122] The time has come for the CDA to cease being a shield to web hosts and for laws to be enacted to address this unacceptable online behavior.

[121] *See* Harper & Mullin, *supra* note 20.

[122] *See Community Standards*, *supra* note 89.