

**THE DISCORD DILEMMA: SECTION 230’S FREE PASS FOR
INTERNET PROVIDERS SANCTIONING ONLINE EXTREMISM**

Claira L. Cooper^{*}

Cite as: Claira L. Cooper, *The Discord Dilemma: Section 230’s Free Pass for Internet Providers Sanctioning Online Extremism*, 32 RICH. J.L. & TECH. 80 (2025).

^{*} Claira L. Cooper is a University of Richmond School of Law J.D. Candidate graduating in 2026. Claira holds a Bachelor’s Degree in Political Science and American Constitutional Studies from Christopher Newport University. This paper was written as a part of an upper-level writing course on terrorism, taught by the amazing Professor Cody Corliss. Thank you to the entire JOLT board for making this publication possible.

ABSTRACT

This Article examines the relationship between the blanket immunity for internet providers guaranteed by Section 230 of the Communication Decency Act and the rise of online extremism on gaming adjacent platforms. This Article analyzes multiple recent events incited by extremists on the gaming platform, Discord, and the real-life consequences that arise when extremism is allowed run rampant on platforms. This Article argues that Section 230, in its current form, enables platforms to turn a blind eye to illegal conduct on their website by avoiding moderation, thus making it clear that Section 230 is in dire need of an update to keep the internet safe for children.

Table of Contents

<i>I. INTRODUCTION</i>	83
<i>II. SECTION 230: LIFE AND LEGACY</i>	84
A. How Does Section 230 Work?	86
<i>II. INTERNET EXTREMISM</i>	87
A. The Discord Leaks	90
B. Discord's Blind Eye	92
<i>III. JUDICIAL SCOPE</i>	98
A. Zeran v. America Online	99
B. Dart v. Craigslist, Inc.	100
C. Doe v. Myspace	101
D. Gonzalez v. Google LLC.....	102
<i>IV. RECOMMENDATIONS</i>	103
A. First Amendment Implications	104
B. Self-Regulation	106
C. State Run Moderation	107
D. Looking to Our Allies.....	109
E. Legislative Carve-Outs	110
<i>V. CONCLUSION</i>	112

I. INTRODUCTION

[1] It has been 30 years since United States Representatives Christopher Cox, R-CA, and Ron Wyden, D-OR, reached across the aisle to pass what is now known as ‘the 26 words that created the internet.’¹ To put that into perspective, the Cox-Wyden Amendment to the Communications Decency Act, presented on the House floor in August of 1995, came a mere two years after the World Wide Web was released into the public domain.² Likewise, the Amendment came one year after the White House created its first website.³ In 1995, there were 16 million people on the internet; meanwhile, today, it is projected that there are 5.56 billion people online.⁴ Despite 30 years of innovation and the internet becoming engrained into virtually every aspect of modern life, that 1995 Amendment, which is now known as the Communications Decency Act, or “Section 230”, is still the primary law of the land regulating life online,⁵ providing a blanket from liability for internet providers.⁶

[2] The following paper will address the ways in which this lack of liability for internet providers comes at the expense of children’s safety online due to the rise of unchecked extremism. This paper will begin with

¹ JEFF KOSSEFF, *THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 2* (Cornell Univ. Press 2019).

² See Julian Ring, *30 Years Ago, One Decision Altered the Course of Our Connected World*, NATIONAL PUBLIC RADIO (Apr. 30, 2023), <https://www.npr.org/2023/04/30/1172276538/world-wide-web-internet-anniversary> [<https://perma.cc/FYE9-NNSD>].

³ *Imagining the Internet’s Quick Look at the Early History of the Internet*, ELON U., <https://www.elon.edu/u/imagining/time-capsule/early-90s/internet-history/> [<https://perma.cc/A5NH-GBTW>].

⁴ *Digital Around the World*, DATAREPORTAL, <https://datareportal.com/global-digital-overview> [<https://perma.cc/46MH-4D83>].

⁵ 47 U.S.C. § 230.

⁶ *Id.*

explaining in more detail how Section 230 works. Next, this paper will discuss internet extremism's unique effect on minors and move into case examples of extremist conduct on the gaming adjacent platform, Discord. This paper will analyze the features of gaming platforms that make these types of sites fertile for extremism and how the protections of Section 230 fail to incentivize platforms to make any meaningful change to promote online safety. This paper will then discuss court cases that have helped reinforce Section 230's free pass to internet platforms and finally, address possible recommendations with considerations towards the first amendment and the importance of life online.

II. SECTION 230: LIFE AND LEGACY

[3] Section 230 was created to solve key issues regarding the internet in 1995, but it does not adequately address the modern-day aspects of life online in 2025. Section 230 was born out of what Representative Cox saw as the legal system providing "a massive disincentive for the people who might best help us control the internet to do so."⁷

[4] In the early 1990s, the State of New York was trying its hand at regulating internet platforms, thus leading to two decisions that troubled lawmakers. In *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, the court allowed summary judgment in favor of CompuServe, Inc., finding that the platform functioned as a distributor, rather than a publisher, due to the fact that it employed a third party to screen content.⁸ CompuServe itself was in no way screening or controlling the content presented on its platform, therefore shielding itself from vicarious liability for the content posted.⁹ Meanwhile, in *Stratton Oakmont Inc. v. Prodigy Servs. Co.*, 1995 N.Y. Misc. LEXIS 712, the court held that the online service provider was liable for the speech of its users because it actively employed screening mechanisms and

⁷ 104 CONG. REC. H8460–70 (daily ed. Aug. 5, 1995) (statement of Rep. Christopher Cox)

⁸ *Cubby, Inc. v. Compuserve, Inc.*, 776 F. Supp. 135, 137–140 (S.D.N.Y. 1991).

⁹ *Id.*

content guidelines.¹⁰ Congress found these two cases to be deterring internet platforms from doing their due diligence to keep the internet safe, as screening could get you punished, and looking the other way protected you from liability.¹¹

[5] The legislative history tells us Congress's vision in the passage of Section 230 spoke directly to these cases, as Representative Cox told the floor, "Mr. Chairman, that is backwards. We want to encourage people like Prodigy, like CompuServe... to do everything possible for us, the customer, to help us control, at the portals of our computer, at the front door of our house, what comes in and what our children see."¹² He suggested that by incentivizing the platforms to regulate themselves by shielding liability for content that may slip through the cracks, it would in turn "make sure that it operates more quickly to solve our problem of keeping pornography away from our kids [and] keeping offensive material away from our kids."¹³

[6] From the very beginning of the internet, encouraging providers to monitor their content was thought to be favorable over government regulation, as the government moves slow, or rather, in the words of the Congressman, "no matter how big the army of bureaucrats, it is not going to protect my kids because I do not think the Federal Government will get there in time."¹⁴ Despite this, it has become clear in recent years that the government's incentive to platforms through Section 230 is not enough to make them safely monitor their sites.¹⁵

¹⁰ *Stratton Oakmont Inc., v. Prodigy Servs. Co.*, 1995 Misc. LEXIS 712, at *2–*5 (N.Y. Sup. Ct. 1995).

¹¹ CONG. REC., *supra* note 7.

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ Kids Online Health and Safety Task Force Announces Recommendations and Best Practices for Safe Internet Use, NAT'L TELECOMM. & INFO. ADMIN., (2024),

[7] A law that, at its inception, was crafted with the internet safety of America's children at its core, is now the first line of defense from civil liability for social media companies and internet platforms who are accused of allowing an assortment of horrific content, including exposing children to extremist propaganda and recruitment.¹⁶ The internet has expanded and innovated in tremendous ways over the past 30 years, and likewise, Section 230 needs to be updated to account for the issues that lawmakers could have never imagined in 1995.

A. How Does Section 230 Work?

[8] Section 230 has allowed the internet to become, for better or worse, what it is today. By declaring that “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider”,¹⁷ Section 230 precludes providers from being held liable for information coming from third-party content.¹⁸ In simpler terms, platforms cannot be sued for the content of their users, whether it be offensive, hateful, or even outright illegal.¹⁹ Without this shield, the internet may look more like a newspaper, with content being entirely provided and vetted by the company it comes from, without interaction by third-party users.²⁰

<https://www.ntia.gov/press-release/2024/kids-online-health-and-safety-task-force-announces-recommendations-and-best-practices-safe-internet> [<https://perma.cc/QNY7-3WR8>].

¹⁶ KOSSEFF, *supra* note 1 at 3–5.

¹⁷ 47 U.S.C. § 230 (c)(1).

¹⁸ VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW (2024).

¹⁹ *See generally* 47 U.S.C. § 230(c)(1); *Dart v. Craigslist, Inc.*, 665 F. Supp. 2d 961, 966 (N.D. Ill. 2009).

²⁰ KOSSEFF, *supra* note 1, at 4.

[9] All of the top ten websites of 2024 benefit from the immunity provided by Section 230 in some way, whether it is social media companies like Facebook, Instagram, or X actively encouraging content provided by its users, Google and other search engines relying on content by third parties, or even Amazon creating a trusted brand by allowing its shoppers to leave reviews on products purchased.²¹ These companies do not have to fear lawsuits for content posted on their platforms, so long as they act in “good faith,” although Section 230(c)(2)(A) fails to define what exactly it means to act in good faith.²² Despite this good faith requirement, Section 230 has, in many cases, prevented victims from suing online platforms even if the platform “encouraged the user to post horrific content and refused to remove it.”²³

[10] Such broad immunity has allowed the internet to become a host to bad actors and criminal activity, as Section 230 in turn protects “terrorist recruitment, online sex trafficking, discriminatory housing sales and vicious harassment,” as many platforms are failing to moderate, turning a blind eye, or even in some cases, encouraging this sort of content.²⁴

II. INTERNET EXTREMISM

[11] The fact that extremists have taken refuge on the internet is not new news.²⁵ Social media has become a large source of recruitment, allowing for institutionalized socialization by spreading narratives and propaganda

²¹ *Id.*

²² 47 U.S.C. § 230(c)(2)(A).

²³ KOSSEFF, *supra* note 1, at 5.

²⁴ *Id.*

²⁵ Robyn Torok, *ISIS and the Institution of Online Terrorist Recruitment*, MIDDLE E. INST. (Jan. 29, 2015), <https://www.mei.edu/publications/isis-and-institution-online-terrorist-recruitment> [<https://perma.cc/Q9HN-LWRN>].

around the world.²⁶ While traditionally the fear was the spread of ISIS, Islamic extremist groups are not the only ones who have taken to the internet and social media to spread propaganda and recruit new members, as right-wing and left-wing extremist groups have weaponized current political and social unrest to amplify their own rhetoric.²⁷

[12] Major social media companies have come into controversy in recent years for their efforts toward removing terrorist content from their platforms, which have been limited to that of U.S.-designated foreign terrorist organizations without monitoring content from domestic groups.²⁸ Critics have gone as far as to accuse social media companies of implicitly permitting right-wing extremists to “operate with impunity” on their platforms.²⁹

[13] The lack of moderation for domestic extremist groups creates a risk to all on the internet, but especially to America’s youth. The U.S. Surgeon General issued an advisory in 2023, warning parents to limit their children’s online consumption, as findings found 95% of minors aged 13-17 years old use at least one social media platform, with more than a third saying they are online “constantly.”³⁰ While most social media platforms in the United States require their members to be at least 13 years of age, nearly 40% of

²⁶ *Id.*

²⁷ Peta Lowe, *Young People and Violent Extremism in the COVID-19 Context*, AUSTL. STRATEGIC POL’Y INST. 101, 102 (2021).

²⁸ Bennett Clifford, *Moderating Extremism: The State of Online Terrorist Content Removal Policy in the United States*, PROGRAM ON EXTREMISM: GEORGE WASH. U. 17 (Dec. 15, 2021), <https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/Moderating%20Extremism%20The%20State%20of%20Online%20Terrorist%20Content%20Removal%20Policy%20in%20the%20United%20States.pdf> [https://perma.cc/ZE33-XK2B].

²⁹ *Id.* at 17.

³⁰ U.S. SURGEON GENERAL’S ADVISORY, SOCIAL MEDIA AND YOUTH MENTAL HEALTH 4 (2023).

children aged 8-12 years old are somehow still on social media.³¹ In 2023, a Gallup survey found that American teens are spending, on average, 4.8 hours a day online.³² A lack of parental monitoring and easy-to-bypass age requirements has allowed America's children unfettered access to the internet.

[14] This nearly constant and unmonitored usage of social media by America's children puts them directly in harm's way as they become exposed to extremist content online.³³ Children's exposure to this type of content affects them differently than adults, as the U.S. Surgeon General warns:

In early adolescence, when identities and sense of self-worth are forming, brain development is especially susceptible to social pressures, peer opinions, and peer comparison. Frequent social media use may be associated with distinct changes in the developing brain in the amygdala (important for emotional learning and behavior) and the prefrontal cortex (important for impulse control, emotional regulation, and moderating social behavior), and could increase sensitivity to social rewards and punishments.

As such, adolescents may experience heightened emotional sensitivity to the communicative and interactive nature of social media.³⁴

[15] Children's online exposure to extremist content has become especially problematic as gaming platforms, which are known to be most

³¹ *Id.* at 4.

³² Jonathan Rothwell, *Teens Spend Average of 4.8 Hours on Social Media Per Day*, GALLUP (Oct. 13, 2023), <https://news.gallup.com/poll/512576/teens-spend-average-hours-social-media-per-day.aspx> [<https://perma.cc/M5VP-4Q6G>].

³³ Lowe, *supra* note 27 at 102.

³⁴ U.S. SURGEON GENERAL'S ADVISORY, *supra* note 30 at 5.

popular with children and teens, see an influx of terrorist and extremist propaganda.³⁵ In fact, the New York University Stern Center conducted a survey finding that as of 2023, 51% of gamers in the top five video game markets had come across some form of extremism while playing multiplayer games in the past year.³⁶

A. The Discord Leaks

[16] Worldwide attention was brought to the gaming industry's relationship with extremism in 2023 when the United States faced one of the biggest leaks of government secrets in history, stemming from a Discord chat of teenaged boys.³⁷ Jack Teixeira, a 21-year-old member of the Massachusetts Air National Guard, took to the chatrooms on the gaming-adjacent platform, Discord, to reveal highly sensitive, classified information.³⁸ Teixeira, known as "OG" in the Discord chatroom filled primarily with juvenile boys sharing extremist ideologies, posted his own written reports and over 300 photos of classified documents.³⁹ These documents included information on detailed charts of battlefield conditions in Ukraine and potential trajectory maps of North Korean ballistic missiles, just to name a small snapshot of the information leaked.⁴⁰

³⁵ *Addressing Extremism in Online Games Through Platform Policies*, AMERICAN DEFAMATION LEAGUE (May 16, 2024), <https://www.adl.org/resources/report/addressing-extremism-online-games-through-platform-policies> [<https://perma.cc/NQ3V-YFCC>].

³⁶ Mariana O. Rosenblat & Paul M. Barrett, *Gaming the System: How Extremists Exploit Gaming Sites and What Can Be Done to Counter Them*, NYU STERN CENTER FOR BUS. & HUMAN RIGHTS (May 2023), https://bhr.stern.nyu.edu/wp-content/uploads/2024/01/NYUCBHRGaming_ONLINEUPDATEDMay16.pdf [<https://perma.cc/PY8H-R8MB>].

³⁷ Patrice Taddonio, *Jack Teixeira Pleads Guilty in 'Discord Leaks' Case*, PBS NEWS (Mar. 4, 2024), <https://www.pbs.org/wgbh/frontline/article/jack-teixeira-guilty-plea-discord-leaks-national-security/> [<https://perma.cc/82R4-FXZG>].

³⁸ *Id.*

³⁹ *See id.*

⁴⁰ *See id.*

[17] Teixeira shared streams of classified information with his fellow extremist friends in the Discord server for months with no issue. It was not until a teenage boy in the chat started to repost the information in other Discord servers, eventually spreading the information to other forms of social media that the FBI caught wind of the situation and began a manhunt for “OG.”⁴¹

[18] Friends shared with the Washington Post that Teixeira shared the government secrets with the group in hopes of impressing the other boys in the chat.⁴² Best said in the words of then-Attorney General Merrick Garland, “Jack Teixeira repeatedly shared classified national defense information on a social media platform in an attempt to impress anonymous friends on the internet – instead, it has landed him a 15-year sentence in federal prison.”⁴³ Jodie Cohen, Special Agent in Charge of the Boston Division of the Federal of Bureau Investigations reported that Teixeira betrayed the country in order to, “boost his ego and impress his friends.”⁴⁴

[19] The Washington Post was able to interview a member of the chatroom, a minor, of whom they had to gain the permission of his mother in order to speak with.⁴⁵ The boy, who described himself as a “young

⁴¹ Shane Harris & Samuel Oakford, *The Discord Leaks, Explained*, WASH. POST, <https://www.washingtonpost.com/national-security/2023/12/11/discord-leaks-documentary/> [<https://perma.cc/VK82-UBXL>] (last updated Dec. 12, 2023).

⁴² *Id.*

⁴³ Press Release, U.S. Attorney’s Office, District of Massachusetts, Former Air National Guardsman Sentenced to 15 Years in Prison for Unlawfully Disclosing Classified National Defense Information (Nov. 12, 2024), <https://www.justice.gov/usao-ma/pr/former-air-national-guardsman-sentenced-15-years-prison-unlawfully-disclosing-classified> [<https://perma.cc/3LD2-8Q5E>].

⁴⁴ *Id.*

⁴⁵ Shane Harris & Samuel Oakford, *Discord Member Details How Documents Leaked from Closed Chat Group*, WASH. POST, <https://www.washingtonpost.com/national->

teenager,” described “OG” as the undisputed leader and chatroom administrator, meaning he was able to control membership.⁴⁶ Other members of the Discord chatroom shared that the young boys saw their secret server as a safe space to make “racist and antisemitic jokes, peddle gory videos and trade conspiracy theories about government agents.”⁴⁷

[20] This begs the question—how could a group of anonymous teenage boys, forming their own extremist oasis online, be behind one of the biggest security leaks in United States history? How is it possible that national security secrets were being published clearly with the standard “SECRET,” “TOP SECRET” classification markings,⁴⁸ indicating that they contained highly classified United States government information for months on end without law enforcement catching wind of it? A major factor of this phenomenon is the way in which sites like Discord are set up, as the sites turn a blind eye to extremists on their platforms and even enable such conduct through their law enforcement evading features.⁴⁹

B. Discord's Blind Eye

[21] Discord's features create fertile grounds for extremist propaganda online, leading to real-life consequences as seen in the Teixeira case. Discord allows its users to create secret chatrooms, preventing outsiders

security/2023/04/12/discord-leaked-documents/ [https://perma.cc/M76N-HN7T] (last updated Apr. 16, 2023).

⁴⁶ *Id.*

⁴⁷ Press Release, U.S. Attorney's Office, District of Massachusetts, *supra* note 43.

⁴⁸ Press Release, U.S. Attorney's Office, District of Massachusetts, *supra* note 43.

⁴⁹ Samuel Oakford et al., *'Problematic Pockets': How Discord Became a Home for Extremists*, WASH. POST, <https://www.washingtonpost.com/national-security/2023/12/12/discord-app-extremism/> [https://perma.cc/4P4C-SVPW] (last updated Dec. 12, 2023).

from being able to see that the channel even exists.⁵⁰ Discord allows for anonymous members to control their chatrooms with virtually no outside oversight, as Discord outsources moderation to unpaid volunteers who are members of the chatrooms themselves.⁵¹ These moderators are tasked with reporting behavior that violates community guidelines, but it seems in practice that this setup is a failure, as Teixeira was moderator of the chatroom, he himself leaked secret information.⁵²

[22] Discord operates under the hopes that “our users play their part by reporting violations—showing they care about this community as much as we do.”⁵³ In an environment where extremism is so prevalent, it becomes unlikely that players will report such behavior. Even when flagged and removed from the platform for conduct violations, it is incredibly simple to create a new account and carry on with the same bad behavior.⁵⁴ The Washington Post reported that according to interviews with current and former employees, the company's “rules and culture allowed a racist and antisemitic community to flourish, giving Teixeira an audience eager for his revelations and unlikely to report his alleged law breaking.”⁵⁵

⁵⁰ Samantha Murphy Kelly, *The Dark Side of Discord for Teens*, CNN, [https://www.cnn.com/2022/03/22/tech/discord-teens/index.html#:~:text=%E2%80%9CWith%20Discord%2C%20you%20subscribe%20to%20channels%20and,Virginia%20who%20focuses%20on%20digital%20privacy%20is%20sues%20\[https://perma.cc/ZAN3-8CY4\]](https://www.cnn.com/2022/03/22/tech/discord-teens/index.html#:~:text=%E2%80%9CWith%20Discord%2C%20you%20subscribe%20to%20channels%20and,Virginia%20who%20focuses%20on%20digital%20privacy%20is%20sues%20[https://perma.cc/ZAN3-8CY4]) (last updated Mar. 22, 2022, at 12:22 PM).

⁵¹ See *id.*; Oakford et al., *supra* note 49.

⁵² Oakford, et al., *supra* note 49.

⁵³ Discord Safety, *Discord Transparency Report: April–Dec 2019*, DISCORD (Mar. 20, 2020), <https://discord.com/blog/discord-transparency-report-april-dec-2019> [https://perma.cc/9LGW-2L92].

⁵⁴ Oakford et al., *supra* note 49.

⁵⁵ Oakford et al., *supra* note 49.

[23] Discord has additional features that make it easy to circumvent law enforcement. Chats can be immediately and permanently deleted, making it impossible to reconstruct at the request of law enforcement.⁵⁶ Additionally, a major issue with the platform is the lack of real-time visibility into users who may be bad actors, “offering time and space [to extremists] ... despite a slew of warning signs missed by the company.”⁵⁷

[24] Discord was known to be a breeding ground for extremism long before the 2023 leaks and failed to implement policies that address these issues. In 2018, Discord was home to the organizers and participants of the Charlottesville “Unite the Right” neo-Nazi rally.⁵⁸ The organizers were able to take advantage of secret chatrooms, using anonymous pin names to plan details from carpools, dress code, lodging and even how to improvise weapons in preparation for the deadly rally.⁵⁹ Prosecutors used the messages recovered from the chat rooms to prove that the organizers intended to incite violence in Charlottesville.⁶⁰ In response to the situation in Charlottesville, Keegan Hanks, an analyst with the Southern Poverty Law Center, told the New York Times that Discord is “a central communication interface for the white nationalist and neo-Nazi movements.”⁶¹

⁵⁶ Oakford et al., *supra* note 49.

⁵⁷ Oakford et al., *supra* note 49.

⁵⁸ Meagan Flynn, *Subpoena for App Called ‘Discord’ Could Unmask the Identities of Charlottesville White Supremacists*, WASH. POST (Aug. 7, 2018), <https://www.washingtonpost.com/news/morning-mix/wp/2018/08/07/subpoena-for-app-called-discord-could-unmask-identities-of-charlottesville-white-supremacists/> [https://perma.cc/VP2V-XRUE].

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ Kevin Roose, *This Was the Alt-Right’s Favorite Chat App. Then Came Charlottesville*, N.Y. TIMES (Aug. 15, 2017),

[25] Discord, while willing to remove illegal content when or if it is flagged, makes sure to remind the community that messages will continue to stay private, as the community guidelines reinforce, “we do not actively monitor and aren’t responsible for any activity or content posted.”⁶² This statement by Discord gives the greenlight to extremists that despite a wave of backlash against the platform, it has not and will not put measures in place to actively monitor chatrooms.

[26] Discord's blind eye towards moderation and permissive features is an ongoing threat to children. In recent months, law enforcement officials across the country have discovered an international network using Discord to target children with a “sadistic form of social media terror”.⁶³ Members now known to be a part of the “764 Terror Network,” as labeled by the Federal Bureau of Investigations, have taken advantage of Discord's anonymity and secret chatrooms to seek out and blackmail children with mental health issues.⁶⁴ This blackmail has led to horrific consequences like minors as young as eight years old, “enga[ging] in and shar[ing] media of self-mutilation, sexual acts, harm to animals, acts of random violence, suicide, and murder, all for the purpose of accelerating chaos,⁶⁵ done via video chat for the entertainment of the extremists on the other end.

<https://www.nytimes.com/2017/08/15/technology/discord-chat-app-alt-right.html>
[<https://perma.cc/DX7R-N5WQ>].

⁶² *Discord's Terms of Service*, DISCORD, <https://discord.com/terms> (last updated Aug. 29, 2025).

⁶³ See Press Release, U.S. Dep’t of Justice, Office of Public Affairs, Member of Violent 764 Terror Network Sentenced to 30 Years in Prison for Sexually Exploiting a Child, <https://www.justice.gov/archives/opa/pr/member-violent-764-terror-network-sentenced-30-years-prison-sexually-exploiting-child> [<https://perma.cc/3QMS-5M4F>] (last updated Feb. 6, 2025).

⁶⁴ *Id.*

⁶⁵ *Id.*

[27] In 2022, a member of the 764 Terror Group, who also happened to be a minor, fatally stabbed an elderly woman while live-streaming the act on Discord for his friends to see.⁶⁶ The Washington Post reports that months prior to the incident, Discord had shut down his account and reported him to authorities, yet he was able to simply create a new account and remain on the platform.⁶⁷ In the United States, multiple affiliates have been arrested and convicted for crimes involving 764's usage of online networks to sexually exploit children.⁶⁸ U.S. Attorney Mark Totten for the Western District of Michigan emphasized this threat after a Michigan man was sentenced to 30 years in prison for his involvement in the group, saying—"This case represents a new and depraved threat against our kids and our communities: violent online extremists who manipulate their minor victims to commit self-harm and create sexually explicit images."⁶⁹

[28] While the Department of Justice has made arrests of specific individuals who are members of these massive online groups, their hands are tied in addressing the social media platforms facilitation of such conduct, likely due to Section 230 of the Communications Decency Act. Lack of government intervention gives social media companies little incentive to change their policies, as despite knowing that extremist content is alive and well on its platform, Discord has not changed any of the features that enable such content to flourish. In failing to do so, Discord and other similar sites are simply standing behind the rights provided to them by our Government via Section 230.

⁶⁶ Shawn Boburg, et al., *On Popular Online Platforms, Predatory Groups Coerce Children into Self-Harm*, WASH. POST (Mar. 13, 2024, at 08:01 ET), <https://wapo.st/4mxHXyl> [<https://perma.cc/XCN7-8JVM>].

⁶⁷ *Id.*

⁶⁸ Press Release, U.S. Dep't of Justice, Office of Public Affairs, *supra* note 65.

⁶⁹ Press Release, U.S. Dep't of Justice, Office of Public Affairs, *supra* note 65.

[29] A law created with the safety of children at its heart is now the shield of liability for companies like Discord, which negligently runs the platform in a way that enables America's children to come into contact with violent, and potentially life-altering forms of extremism.⁷⁰ In 1995, the nation's legislature feared children coming into contact with pornography on the internet—they could have never guessed what horrific media awaits their children in 2025.⁷¹

[30] Parents have noticed the impact on their children and have tried to take it into their own hands. In February of 2025, a complaint was filed in the Superior Court of the State of California, County of San Mateo, against Discord, in addition to another gaming platform, Roblox.⁷² The Plaintiffs assert that the victimization and sexual exploitation of a minor child online was possible only because of the egregious conduct of the two sites.⁷³ Amongst the claims are both negligence and strict liability claims for failure to warn and unreasonable design.⁷⁴ The complaint demands: “There are steps Roblox and Discord could take to protect children and make their apps safer. But time and again, they have refused to invest in basic safety features to protect against exactly the kind of exploitation Plaintiff suffered here.”⁷⁵

⁷⁰ See 104 CONG. REC. H8460–70 (daily ed. Aug. 5, 1995) (statement of Rep. Christopher Cox). (noting that in New York, an online service provider could be held liable for defamation after the provider advertised itself as a family-friendly network exercising a greater control over offensive material on its platform).

⁷¹ See *id.* at 8470 (discussing the problem of computer-literate children having untraceable access to pornographic material through online computer services).

⁷² Complaint at 1, *John Doe v. Roblox Corp.*, No. 25-CIV-01193 (Super. Ct. Cal. filed Feb. 13, 2025).

⁷³ *Id.* at 1.

⁷⁴ *Id.* at 92, 96.

⁷⁵ *Id.* at 1.

[31] As of September 2025, an additional lawsuit has been filed in the Superior Court of California, County of San Francisco accusing Roblox and Discord of “recklessly and deceptively operating their business in a way that led to the sexual exploitation and suicide” of a 15-year-old California boy.⁷⁶ The minor took his own life after being “groomed and coerced to send explicit images” on the two apps.⁷⁷ Notably, “the suit alleges the two apps misrepresented safety on their platforms, asserting that the design of the apps ‘makes children easy prey for pedophiles’ due to a lack of safeguards and predator screening.”⁷⁸

[32] Unfortunately, this complaint is unlikely to go far. Cases involving Section 230 have been consistently unfavorable towards plaintiffs, as courts have given substantial deference to the 1995 Amendment, allowing platforms to avoid liability for harmful, indecent, and even illegal behavior. Section 230, in its current form, is preventing any real moderation of platforms, likewise leaving America’s children and teens at risk. This paper will now turn to the Judicial Scope of Section 230 to address the contours of the law.

III. JUDICIAL SCOPE

[33] While there have been a plethora of court cases involving Section 230 in the 30 years since its inception, many questions remain about the law’s meaning and scope. Courts, particularly the Supreme Court, have been troubled by Section 230 and what to do with cases involving the

⁷⁶ Marlene Lenthang & Austin Mullen, *Roblox, Discord Sued after 15-year-old boy was Allegedly Groomed Online Before He Died by Suicide*, NBC NEWS, <https://www.nbcnews.com/news/us-news/roblox-discord-sued-15-year-old-boy-was-allegedly-groomed-online-died-rcna231049> [<https://perma.cc/95ZB-PREH>] (last updated Sept. 13, 2025, at 22:47 ET).

⁷⁷ *Id.*

⁷⁸ *Id.*

internet more generally, as best said by Justice Kagan during oral arguments of *Gonzales v. Google*, “we don’t really know about these things. You know, these are not like the nine greatest experts on the internet.”⁷⁹ Likewise, that confusion leads to a heavy difference to Congress, creating a very expansive interpretation of the law. The court's interpretation has upheld immunity to service providers who allow harassment, illegal activity, and even terrorism to run rampant on their platforms.

A. *Zeran v. America Online*

[34] The first case interpreting Section 230 reached the Fourth Circuit when an anonymous user posted Kenneth Zeran’s name and telephone number to AOL’s electronic bulletin board, advertising memorabilia with slogans that glorified the 1995 Oklahoma City Bombing, in which 168 people died.⁸⁰ Zeran began to receive threatening phone calls from people outraged by the bulletin.⁸¹ Zeran sued American Online, claiming negligence in allowing the bulletin posts to remain and reappear on their website, despite having received several complaints from Zeran.⁸² The Fourth Circuit ruled that “the CDA preempts a negligence cause of action against an interactive computer service provider arising from that provider's distribution of allegedly defamatory material provided via its electronic bulletin board.”⁸³ This case was the first of its kind, strongly protecting Section 230 by asserting that there is broad federal immunity to any cause of action that would make service providers liable for information coming

⁷⁹ Alan Z. Rozenshtein, *Interpreting the Ambiguities of Section 230*, BROOKINGS (Oct. 26, 2023), <https://www.brookings.edu/articles/interpreting-the-ambiguities-of-section-230/> [<https://perma.cc/LR9P-2C2Y>].

⁸⁰ *Zeran v. America Online*, 958 F. Supp. 1124, 1127 (E.D. Va. 1997).

⁸¹ *Id.* at 1126.

⁸² *Id.* at 1126.

⁸³ *Id.* at 1137.

from a third-party user, even when the company has notice of an issue and chooses not to address it.⁸⁴ The impact of this case allows platforms like Discord to avoid liability for claims of negligence when its features allow bad acts to go on unchecked on their sites.

B. Dart v. Craigslist, Inc.

[35] The Sheriff of Cook County, Illinois, sued Craigslist, alleging that the site's "erotic services" section facilitated prostitution and created a public nuisance, due to all of the crimes the Sheriff's Office had to respond to related to Craigslist.⁸⁵ The Sheriff argued that Craigslist went beyond being a traditional publisher or intermediary because it induces users to post ads involving criminal conduct by having the "erotic services" section and enabling users to search for such services by sexual preferences.⁸⁶ The United States District Court for the Northern District of Illinois held that Craigslist was immune under Section 230, because Craigslist did not create the illegal ads themselves, as the Court held "intermediaries are not culpable for 'aiding and abetting' their customers who misuse their services to commit unlawful acts".⁸⁷ It is important to note that Craigslist's "terms of use" prohibited posting unlawful content.⁸⁸ Likewise, this case makes it clear that even if platforms have features that may suggest illegality or streamline it, the companies still have Section 230 so long as the company itself is not posting the illegal ads or engaging in illegal content creation.⁸⁹ Similarly, Discord's terms of service directly ban "the presence or activities of violent extremist organizations and other violent groups. Users are not

⁸⁴ See generally Zeran, 958 F. Supp. 1124.

⁸⁵ Dart v. Craigslist, Inc., 665 F. Supp. 2d 961 (N.D. Ill. 2009).

⁸⁶ *Id.* at 962.

⁸⁷ *Id.* at 967.

⁸⁸ *Id.* at 962.

⁸⁹ *Id.* at 967–69.

allowed to use Discord to organize, promote, or support violent extremist activities or beliefs”⁹⁰, yet its features enable illegal conduct. As long as Discord itself does not directly post extremist conduct, it is completely covered from liability.

C. Doe v. Myspace

[36] In the Summer of 2005, a thirteen-year-old girl created a Myspace account claiming she was 18, allowing her to circumvent all safety features of the website.⁹¹ A 19-year-old man was able to initiate contact with the girl, and the two met in person, where he sexually assaulted her.⁹² The girl’s mother sued Myspace for failing to implement basic safety measures to prevent sexual predators from communicating with minors on its website.⁹³ The District Court held that Section 230 shields Myspace from liability for actions of its users and additionally found that a party has no legal duty to protect another from the criminal acts of a third person or to control the conduct of another.⁹⁴ The Fifth Circuit affirmed, finding that Section 230 offers immunity for online services broadly in all cases arising from the publication of user-generated content.⁹⁵ With that being said, this case institutionalized that platforms do not need to take reasonable actions to protect children from harm, besides making them affirm their age, allowing

⁹⁰ *Violent Extremism Policy Explainer*, DISCORD (Aug. 29, 2025), <https://discord.com/safety/violent-extremism-policy-explainer> [<https://perma.cc/2TCG-USMT>].

⁹¹ Doe v. Myspace, 629 F. Supp. 2d 663, 664 (E.D. Tex. 2009).

⁹² *Id.*

⁹³ *Id.*

⁹⁴ *Id.*

⁹⁵ *Id.*

sites like Discord to avoid liability without implementing basic safety measures to keep children safe.

D. Gonzalez v. Google LLC

[37] The Supreme Court addressed Section 230 for the first time in 2022, leaving attorneys and Silicon Valley perhaps more confused on the status of Section 230 than they were prior to the highest court's review. Nohemi Gonzalez, a US citizen, was killed by a terrorist attack in Paris, France, in 2015.⁹⁶ Her father sued, claiming that as Google's computer algorithms suggest content to users based on viewing history, it assists ISIS in spreading its message, thus aiding and abetting international terrorism by failing to take meaningful or aggressive action to prevent terrorists from using its services.⁹⁷

[38] The suit circles around the question of whether Section 230(c)(1) immunizes algorithms when it makes targeted recommendations of information provided by another information content provider.⁹⁸ The Court declined to reach the question presented, vacated the judgment of the lower court, and remanded for further proceedings consistent with that opinion.⁹⁹ The practical effect of the remand was the dismissal of Gonzalez's claim, and likewise, the question of whether Section 230 covers algorithms is still unknown.

[39] *Twitter, Inc. v. Taamneh*, 598 U.S. 471, (2023) stems from the same facts as *Gonzales*, but focuses on the question of whether Google, Twitter, and Facebook are aiding and abetting international terrorists by "failing to take meaningful or aggressive action to prevent terrorists from using its

⁹⁶ *Gonzalez v. Google LLC*, 598 U.S. 617, 619–20 (2023).

⁹⁷ *Id.* at 619–21.

⁹⁸ *Id.* at 621.

⁹⁹ *Id.* at 622.

services” under 18 U.S.C. 2333.¹⁰⁰ The court found that the social media sites did not “knowingly” provide substantial assistance under 18 U.S.C. 2333 merely because they allegedly *could have* taken more meaningful or aggressive action to prevent such use.¹⁰¹ While this case does not directly address the scope of Section 230, the Supreme Court sets forth that social media companies cannot be said to be aiding and abetting terrorists simply because they did not do enough to prevent them from using the website.¹⁰²

[40] Section 230, as written and interpreted by courts, is unworkable in its current state to address the impacts of extremism online. As the cases above demonstrate, even the most damning and heinous causes of action are not enough for Courts to demand that social media companies raise the bar in terms of content moderation and enforcement. It is clear that Section 230 needs to be updated in alignment with the struggles of modern-day internet usage in order to make the world online safer for our children.

IV. RECOMMENDATIONS

[41] It has been 30 years since the passage of Section 230 and thus the launch of the World Wide Web¹⁰³, making the legislation well overdue for an update. The internet has a nearly infinite capacity, constantly growing and changing. Life online now has real-life consequences, yet in many cases, law enforcement officials find themselves with their hands tied, as Section 230 protects internet providers from liability, even in cases in which the platform's features directly or indirectly lead to harm.¹⁰⁴ When assessing how to revise a question of such monumental reach and importance, the

¹⁰⁰ Twitter, Inc. v. Taamneh, 598 U.S. 471 (2023).

¹⁰¹ *Id.* at 497.

¹⁰² *Id.* at 499–500.

¹⁰³ KOSSEFF, *supra* note 1, at 2.

¹⁰⁴ Aaron Terr, *Why Repealing or Weakening Section 230 is a Very Bad Idea*, FOUND. FOR INDIVIDUAL RTS. & EXPRESSION (Feb. 20, 2023), <https://www.thefire.org/news/why-repealing-or-weakening-section-230-very-bad-idea> [<https://perma.cc/7JXJ-F6CB>].

question of how to fix it is easier said than done.

A. First Amendment Implications

[42] While this paper has highlighted the negative implications of Section 230, it cannot go without mentioning the law's importance to society as we know it. Section 230 is a major safeguard of free speech on the internet and repealing it completely would likely lead to less expressive freedom and viewpoint diversity online, as many platforms would likely stop allowing user-generated content, and those that continued to would open themselves up to an endless cycle of litigation.¹⁰⁵

[43] While the focus of this paper is not on the freedom of speech, it is crucial to know what the First Amendment protects and what it does not protect online. The incitement of violence has never been protected under the First Amendment, yet Section 230 shields platforms from facing any civil liability for such content when it is posted, and even when its features enable this speech by design or amplification.¹⁰⁶

[44] Critics find protection for platforms especially concerning due to the business models of major platforms, as most revenue is ad-driven, leading platforms to optimize engagement at the “expense of democratic discourse”.¹⁰⁷ Allison Stanger, a fellow at the Harvard Kennedy School Ash Center for Democratic Engagement and Innovation, makes it clear that the amplification of harmful content on the internet is “a product, not a public service”.¹⁰⁸ Nonetheless, even if the mindset is profit-driven, rather than

¹⁰⁵ *See id.*

¹⁰⁶ Jaron Lanier et al., *Sunset and Renew: Section 230 Should Protect Human Speech, Not Algorithmic Virality*, HARV. KENNEDY SCH. ASH CTR. (Oct. 30, 2024), <https://ash.harvard.edu/articles/sunset-and-renew-section-230-should-protect-human-speech-not-algorithmic-virality/> [<https://perma.cc/KAS3-4VCV>].

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

rights-based, it does not change the fact that there are serious First Amendment implications when it comes to Section 230 and internet speech.

[45] In shaping a working solution to the issue of extremists on the internet, it is important to consider *Reno v. ACLU*, 521 U.S. 844 (1997). In this case, the Supreme Court struck down two provisions of the Communications Decency Act, which were enacted to protect minors from communications online, making it so any platform that “knowingly permits any telecommunications facility under his control” that is considered to be “indecent” and “patently offensive” could face up to two years in prison.¹⁰⁹ The Supreme Court held that the ambiguities of the law's scope violated the First Amendment, with a major issue being the fact that the government did not define “indecent” or “patently offensive”, provoking uncertainty amongst speakers on how the two relate.¹¹⁰ The Court held that the statute “unquestionably silences some speakers whose messages would be entitled to constitutional protection... The CDA’s burden on protected speech cannot be justified if it could be avoided by a more carefully drafted statute.”¹¹¹

[46] While this case appears problematic for the purposes of this paper, it is important to remember how fundamentally different the threat was in 1997, compared to our modern day. Justice Stevens defended the decision to strike down the provisions protecting children online by writing that, in reference to pornography, “users seldom encounter such content accidentally. ‘A document's title or description of the document will usually appear before the document itself... almost all sexually explicit images are preceded by warnings as to the content.’”¹¹² It is common knowledge today that nicely named files explaining the content you are about to see are no longer the norm when something is sent over chatrooms like Discord, or

¹⁰⁹ *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 871–72 (1997).

¹¹⁰ *Id.*

¹¹¹ *Id.* at 874.

¹¹² *Reno*, 521 U.S. at 854.

even publicly on your X or Facebook feed, as the way content is shared is drastically different with the rise of social media. Additionally, this amendment to Section 230 created criminal liability for platform owners, not just merely revoking the liability protections from platforms, thus making the lack of definition of key terms especially concerning as someone's liberty could be at stake.¹¹³ Nonetheless, the implications of *Reno* make it clear that any alteration to Section 230 needs to be done with the utmost precision.

B. Self-Regulation

[47] One consideration to take into mind before drafting legislation is sources of non-legal regulation. Most major social media providers in the U.S. are publicly traded companies, therefore having obligations to shareholders who are concerned with extremist and terrorist usage of their platforms.¹¹⁴ Illegal activity linked to platforms causes a public relations crisis and a possible downturn in stock prices, giving platforms, in theory, reason to keep this sort of content off their sites.¹¹⁵

[48] In 2019, the world saw a first-of-its-kind “self-regulation” by major social media companies, as Facebook, Google, and Twitter all joined the “Christchurch Call”, a voluntary pledge in an effort to prevent harmful content from going viral.¹¹⁶ The social media giants joined the pledge after a deadly attack of a mosque, which was inspired by hateful online content, left 51 people dead and heightened global fears that, “Facebook, Google and Twitter have become conduits for terrorism, unable to keep pace with

¹¹³ Terr, *supra* note 104.

¹¹⁴ Clifford, *supra* note 28, at 6.

¹¹⁵ *Id.* at 7.

¹¹⁶ Tony Romm & Drew Harwell, *Facebook, Google Will Join New Zealand in International Pact Against Online Extremism, While White House Remains Undecided*, WASH POST. (May 14, 2019), https://www.washingtonpost.com/business/economy/trump-adviser-will-attend-paris-conference-on-social-media-abuse/2019/05/14/2edb2fec-7691-11e9-b7ae-390de4259661_story.html [<https://perma.cc/AMR8-7VAT>].

malicious actors who've proven deft at evading Silicon Valley's efforts to prevent harmful content from going viral on the Web."¹¹⁷

[49] While the Christchurch Call shows platforms may be responsive to public opinion, this overestimates the ability of smaller platforms. Social media magnates, like Facebook, Google, and Twitter, perhaps have more resources to hire review teams, deploy algorithmic detection, and bring in expertise on terrorism and extremism; meanwhile, "smaller entities may lack the will, the resources or the wherewithal to employ removal efforts, creating the commons problem."¹¹⁸

[50] While Discord has seen a surge of popularity in recent years, it is not on the same level as the social media giants, who have the resources to make substantial changes in response to public opinion. While Discord has recently entered talks concerning becoming a publicly traded company, it is currently privately owned.¹¹⁹ If the platform does become publicly traded, perhaps it will increase its safety features. On the other hand, expecting platforms to adhere to industry norms via their own good will, rather than laws enforcing such norms, gives no incentive to smaller platforms with fewer resources or those that simply don't have the desire to adhere. Likewise, self-regulation on its own is not a suitable solution and provides no assurance that any true moderation will actually happen, but the force of industry norms and public opinion can certainly work alongside meaningful legislation to help solve this issue.

C. State Run Moderation

[51] Another consideration is the government moderating internet

¹¹⁷ *Id.*

¹¹⁸ *See id.*

¹¹⁹ Lauren Hirsch & Mike Isaac, *Discord in Early Talks with Bankers for Potential I.P.O.*, N.Y. TIMES (Mar. 5, 2025), <https://www.nytimes.com/2025/03/05/technology/discord-ipo.html> [<https://perma.cc/276M-G358>].

platforms itself. The U.S. government has always deferred online content moderation to media companies¹²⁰ and that should not change. To bring content moderation now within the direct power of the government would be impractical and unreasonable for multiple reasons. First, the government does not have the resources to take on this responsibility, as it would bring a massive number of new agencies and departments tasked with regulating content, as well as charged with monitoring the legal, ethical and constitutional considerations of any decision made.¹²¹ Second, there is the fear of political abuse, as it is not hard to imagine a world where an administration may simply filter out viewpoints that do not align with its greater policy perspectives.

[52] In 2020, the State of Texas attempted to get involved more directly with content regulation.¹²² The state passed a law prohibiting social media platforms from regulating users' content and mandating disclosure requirements when content was taken down, as in the wake of the 2020 election, Texas saw companies as "fomenting a dangerous movement to silence conservatives."¹²³ Justice Kagan wrote in the majority opinion that the state cannot:

*prohibit speech to improve or better balance the speech market. On the spectrum of dangers to free expression, there are few greater than allowing the government to change the speech of private actors in order to achieve its own conception of speech nirvana. That is why we have said in so many contexts that the government may not 'restrict the speech of some elements of our society in order to enhance the relative voice of others.'*¹²⁴

[53] In reversing and remanding the case, the Supreme Court emphasized

¹²⁰ Clifford, *supra* note 28, at 9.

¹²¹ Clifford, *supra* note 28, at 9.

¹²² *Moody v. NetChoice, LLC*, 603 U.S. 707, 741 (2024).

¹²³ *Id.*

¹²⁴ *Id.* at 741–42.

that social media content moderation is subject to First Amendment protections. This case makes it very clear that government involvement in moderation online is judged on a similar basis to the government restricting speech in other ways, creating a high bar of individual liberties and bringing in substantial constitutional considerations. Considering the heavy obligations the government has towards individual liberties protected by the Bill of Rights, the government likely has less leeway to moderate online activity than private companies would.¹²⁵ Likewise, government regulation of the internet is not only impractical and unreasonable, but also in many cases, unconstitutional.

D. Looking to Our Allies

[54] In recent years, European nations have reacted to the threat of online extremism and terrorism by putting more stringent regulations on social media platforms. Germany passed a law in 2017 requiring social media providers to delete terrorist or other illegal content within 24 hours of it being posted, or else face a five million euro fine.¹²⁶ Meanwhile, the United Kingdom created criminal penalties, making it a chargeable offense for those accessing or viewing terrorist content online.¹²⁷ Likewise, platforms that exist on a multinational scale are often met with much stricter regulations in other jurisdictions than they face in the United States.¹²⁸

[55] These regulations have also been problematic, though, as smaller social media companies, as recently mentioned, often do not have the resources to keep up with compliance.¹²⁹ Additionally, governments adopting such stringent regulations are forced to define the terms of their

¹²⁵ *Id* at 732.

¹²⁶ Clifford, *supra* note 28, at 12.

¹²⁷ Clifford, *supra* note 28, at 12.

¹²⁸ Clifford, *supra* note 28, at 13.

¹²⁹ Clifford, *supra* note 28, at 13.

regulation, which doesn't allow the flexibility to confront new and emerging threats, or otherwise leaves companies with unclear definitions, creating uncertainty on how to comply.¹³⁰ Unfortunately, another cost of increased regulation is nations using them to crack down on political opponents' online speech.¹³¹

E. Legislative Carve-Outs

[56] While Section 230 reform is a convoluted issue, the research points to legislation incentivizing online platforms to better address illicit content themselves as the most viable means. In 2020, the Justice Department, led by Attorney General William Barr, outlined several areas “Ripe for Section 230 Reform”, in which the DOJ proposed carve-outs for Bad Samaritans, Child Abuse and Terrorism, in addition to a case-specific carve-out for actual knowledge.¹³² The Bad Samaritan carve out circles back to the original purpose of Section 230 immunity—that is, to incentivize platforms to conduct responsible moderation; taking away such immunity from platforms that purposefully promote or facilitate content that violates criminal law is an attractive option, but this would require the government to develop precise definitions of a “good” versus “bad” Samaritan.¹³³ Likewise, the carveouts for Child Abuse and Terrorism would open the door for victims to seek civil redress for causes of action we have seen struck down in cases like *Myspace* and *Gonzalez*, though it would require the United States Government to come up with a succinct definition for terrorism, which is no simple task.¹³⁴

¹³⁰ Clifford, *supra* note 28, at 12.

¹³¹ Clifford, *supra* note 28, at 13–14.

¹³² U.S. Dep't of Just., *Department of Justice's Review of Section 230 of the Communications Decency Act of 1996*, DOJ (2020), <https://www.justice.gov/archives/ag/departments-justice-s-review-section-230-communications-decency-act-199> [<https://perma.cc/44PE-6QEL>].

¹³³ See *Twitter, Inc. v. Taamneh*, 598 U.S. 471, 499, 502–03 (2023).

¹³⁴ See *Gonzalez v. Google LLC*, 598 U.S. 617, 621–22 (2023).

[57] The Justice Department also suggested replacing vague terminology and providing a definition for what is meant by “Good Faith”.¹³⁵ The DOJ wanted lawmakers to replace the catch-all at the end of Section 230 (c)(2) reading, “otherwise objectional language” with “unlawful” and “promotes terrorism,” likewise removing some of the blanket immunity for moderation decisions and limiting platforms’ ability to remove content arbitrarily.¹³⁶ Likewise, the DOJ wanted to define “good samaritan” in a way that “would limit immunity for content moderation decisions to those done in accordance with plain and particular terms of service and accompanied by a reasonable explanation, unless such notice would impede law enforcement or risk imminent harm to others.”¹³⁷ Clearly, the former Attorney General’s recommendations did not go very far, as five years later, there has been no meaningful change to Section 230, but the suggestions outlined seem to be working in the right direction.

[58] Another recommendation proposed by experts is to engrain a Duty of Care standard into Section 230, “holding social media platforms responsible for how their sites are designed and created.”¹³⁸ In many ways, this seems like common sense, demanding companies take steps to improve their platforms when the way it functions is allows something illegal to take place directly under its nose. Some have expressed intertwining a duty of care standard into Section 230 by adding a Reasonableness Standard Amendment, revoking immunity upon an inability to show that the platform met its standard of care.¹³⁹ Likewise, this standard would be left to

¹³⁵ U.S. Dep’t of Just., *supra* note 134.

¹³⁶ U.S. Dep’t of Just., *supra* note 134; 47 U.S.C. § 230(c)(2)(A).

¹³⁷ U.S. Dep’t of Just., *supra* note 134.

¹³⁸ Michael D. Smith & Marshall W. Van Alstyne, *It’s Time to Update Section 230*, HARV. BUS. REV. (Aug. 12, 2021), <https://hbr.org/2021/08/its-time-to-update-section-230> [<https://perma.cc/2Y4R-SNDE>].

¹³⁹ Samuel Won, *A More Reasonable Section 230 of the CDA: Imposing a Pre-Defined Duty of Care Requirement on Online Platforms*, 57 GA. L. REV. 1413, 1432 (2023).

substantial judicial discretion to handle on a case-by-case basis and additionally, require a pre-defined definition of what counts as ‘reasonable’ when it comes to online moderation.¹⁴⁰

V. CONCLUSION

[59] In 2021, Mark Zuckerberg, CEO of Facebook, testified before Congress that, “instead of being granted immunity, platforms should be required to demonstrate that they have systems in place for identifying unlawful content and removing it,”¹⁴¹ and further that, Facebook “would benefit from clearer guidance from elected officials.”¹⁴² Even Christopher Cox, one of the architects of the 1995 Amendment to Section 230, has advocated for rewriting it, saying that “the original purpose of this law was to help clean up the Internet, not to facilitate people doing bad things on the Internet.”¹⁴³ It is clear that the nation is coming to a consensus that change needs to happen.

[60] While the internet seems in and of itself infinite, ideas on how to regulate it seem endless as well, each with its own benefits and drawbacks. It is clear that even the smallest change to Section 230 could have substantial implications on the ways in which life online is conducted. The solution on how to reform Section 230 to better protect children from extremism online is not clear today, but it is pertinent that our legislatures

¹⁴⁰ *Id.* at 1418.

¹⁴¹ Dylan Byers, *Zuckerberg Calls for Changes to Tech’s Section 230 Protections*, NBC NEWS, <https://www.nbcnews.com/tech/tech-news/zuckerberg-calls-changes-techs-section-230-protections-rcna486> [<https://perma.cc/GH2V-FBWP>] (last updated Mar. 24, 2021, at 10:11 ET).

¹⁴² Smith & Van Alstyne, *supra* note 140.

¹⁴³ Alina Selyukh, *Section 230: A Key Legal Shield for Facebook, Google is About to Change*, NPR (Mar. 21, 2018, at 05:11 ET), <https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change> [<https://perma.cc/7CPH-F9HV>].

take this issue seriously, engaging in conversations with media companies on how to find a workable way to protect America's children.