Social Media on Trial: How the Supreme Court Could Permanently Alter the Future of the Internet by Limiting Section 230's Broad Immunity Shield

J. Tyler Wampler
Citations:
Please note: citations are provided as a general guideline. Users should consult their preferred
citation format's style manual for proper citation formatting.

Bluebook 21st ed.

ALWD 7th ed.
J. Tyler Wampler, Social Media on Trial: How the Supreme Court Could Permanently Alter the Future of the Internet by Limiting Section 230's Broad Immunity Shield, 90 Tenn. L. Rev. 299 (2023).

APA 7th ed.

Chicago 17th ed.

J. Tyler Wampler, "Social Media on Trial: How the Supreme Court Could Permanently Alter the Future of the Internet by Limiting Section 230's Broad Immunity Shield" (2023) 90:2 Tenn L Rev 299.

AGLC 4th ed.
J. Tyler Wampler, 'Social Media on Trial: How the Supreme Court Could Permanently Alter the Future of the Internet by Limiting Section 230's Broad Immunity Shield' (2023) 90(2) Tennessee Law Review 299

MLA 9th ed.

OSCOLA 4th ed.
J. Tyler Wampler, 'Social Media on Trial: How the Supreme Court Could Permanently Alter the Future of the Internet by Limiting Section 230's Broad Immunity Shield' (2023) 90 Tenn L Rev 299

Provided by:
University of Tennessee College of Law Joel A. Katz Law Library
SOCIAL MEDIA ON TRIAL: HOW THE SUPREME COURT COULD PERMANENTLY ALTER THE FUTURE OF THE INTERNET BY LIMITING SECTION 230'S BROAD IMMUNITY SHIELD

J. TYLER WAMPLER*

INTRODUCTION.................................................................300
I. BACKGROUND ............................................................................302
  A. The Early Internet .................................................................302
  B. The Creation of Section 230.............................................307
  C. Interpreting Section 230 and Its Modern Rules .............310
     1. Section 230's Broad Liability Shield .........................310
     2. The Gradual Limiting of Section 230 Immunity ..........315
  D. Section 230 and Its Dissenters .......................................317
II. SECTION 230 GETS ITS DAY IN COURT: GONZALEZ V. GOOGLE ........................................320
III. POTENTIAL OUTCOMES IN GONZALEZ AND THE RESULTING FALLOUT ........................................329
  A. The Nuances of the Gonzalez Case: Attenuated Causation, Stale Facts, and an Aging Bench .............................329
  B. What We Know About the Justices Individually and Cumulatively .................................................................332
     1. Justice Clarence Thomas..............................................333
     2. Justice Neil Gorsuch .....................................................333
     3. Chief Justice John Roberts and Justices Amy Coney Barrett and Brett Kavanaugh ........................................334
     4. Justices Ketanji Brown Jackson and Elena Kagan .......335
     5. General Confusion on the Bench ..................................336
     6. A Hesitancy to Engage in Activism .............................338
  C. Potential Outcomes in Gonzalez and the Resulting Fallout ..................................................................................339
     1. The Court Guts or Limits Section 230 Immunity: The Truman Show Versus a Horror Show ........................................339
     2. The Court Upholds Broad Section 230 Immunity ......344
     3. Remand: The Court May “Kick the Can Down the Road” .................................................................345
  D. The Gonzalez Decision Will Not Resolve the Dispute Over Section 230: Moody and Paxton ........................................346
  E. Potential Solutions Moving Forward ......................................350
CONCLUSION..................................................................................352
Section 230 of the Communications Decency Act has allowed the internet to develop and flourish at an unprecedented pace. The law has been interpreted broadly to grant immunity to interactive computer services—like social media platforms—from liability for content posted by users. Wielding this immunity, internet platforms are empowered to act innovatively without fear of frivolous lawsuits. However, there are ongoing concerns that this broad interpretation shields modern tech companies from liability for actions that were never intended to be protected.

Two companion cases interpreting Section 230 are currently before the U.S. Supreme Court, where the Court is being asked to decide if social media sites are immunized for liability resulting from the content that their algorithms recommend to users. These will be the first cases in which the Supreme Court will interpret Section 230 at all. The outcome could have drastic consequences for the future of the internet and social media, including stifling free speech and expression. Due to the numerous concerns about shielding tech companies from liability and rapidly advancing AI technology, these cases will not put the issue to rest. Congress must act with haste to step in and clarify the scope of Section 230 immunity.

INTRODUCTION

Section 230(c)(1) is referred to as “the twenty-six words that created the internet.”1 When Senator Ron Wyden and Representative Chris Cox ushered Section 230 through Congress, they were acting in response to an inadequate body of law that applied to the burgeoning internet platforms of the early 1990’s.2 Undoubtedly, they understood that the new law would be important to the future development of cutting-edge technology.3 However, they likely had no clue that the law they were championing would arguably do more to push America into the internet age than any other law in existence.4 Indeed, Section

---

1. JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (Cornell Univ. Press ed., 2019) [hereinafter 26 WORDS]. Mr. Kosseff, who coined the term, is an expert in cybersecurity and Section 230 matters and is a professor of law at the U.S. Naval Academy. His book on Section 230 is a well-informed recounting of the history of the law and it provided the early foundation for much of my research for this article.
2. See infra notes 56-60.
3. See infra notes 56-60.
4. See infra notes 84.
230 is partly responsible for the development of the massive social media platforms that dominate our world today and for America’s primacy as the center of the technology universe.\(^5\)

Section 230(c)(1) states 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.”\(^6\) This has been interpreted broadly to grant interactive computer services—like Twitter, Facebook, and Google—strong immunity to lawsuits for content posted on their platforms by users.\(^7\) Its companion provision, subsection (c)(2), states that no interactive computer service shall be liable for good faith actions taken to moderate user content that the site deems objectionable.\(^8\) Essentially, this empowers social media platforms to moderate user content and deplatform those who violate the terms of service.\(^9\) Taken together, these statutes formed the sword and shield that would drive internet dominance in the modern age, as internet firms were able to act innovatively without fear of liability.\(^10\)

However, despite its importance to the modern world, many groups openly criticize the broad powers contained in Section 230.\(^11\) They argue that Section 230 has been interpreted too broadly and that it shields modern tech companies from liability for acts that were never intended to be protected.\(^12\) Today, two companion cases interpreting §§ (c)(1)’s broad liability shield sit before the U.S. Supreme Court, awaiting a decision of first issue for SCOTUS.\(^13\) The court is being asked to decide whether social media sites are immunized for liability resulting from the content that their algorithms recommend to users, such as “next up” video recommendations on YouTube.\(^14\) More specifically, the court is being asked if YouTube and Twitter have immunity when their algorithms recommended ISIS content to radical jihadists who murdered innocent victims.\(^15\) On its face, this issue appears limited in scope to the facts. However, the fallout from the court’s decision could be

\(^5\) See infra notes 81–88.
\(^7\) See infra Section I.C.
\(^8\) 47 U.S.C.A. § 230(c)(2) (West).
\(^9\) See infra Section I.D.
\(^10\) See infra notes 81–88.
\(^11\) See infra Section I.D.
\(^12\) See infra Section I.D.
\(^13\) See infra Section II.
\(^14\) See infra Section II.
\(^15\) See infra Section II.
drastic. Algorithms are everywhere and they are absolutely necessary if the internet is to continue functioning as it does today.\textsuperscript{16} Imposing liability for algorithmic recommendations would mean that companies are forced—out of fear of limitless exposure to lawsuits—to either (1) restrict any content that seems objectionable at all or (2) restrict absolutely no content.\textsuperscript{17} This would turn the internet into a hellscape of over-moderation, where free speech and expression are stifled, and under-moderation, where literally anything goes.

In this article I begin in Part I by examining the background of Section 230, from its purpose and inception to the modern-day controversies surrounding the law. Then, in Part II, I brief, in detail, the Gonzalez and—to a lesser extent Taamneh—cases that are currently before the Supreme Court. Next, in Part III, I review all the potential outcomes in the companion cases and their potential fallout, including an in-depth assessment of what the court is likely to do and the resulting consequences. I conclude with the thesis that a decision limiting Section 230 liability is inappropriate in this case because, not only do the law and facts lead to a separate conclusion, but the resulting fallout would be dystopian. Finally, I explain that, regardless of whatever happens with these cases in the coming months, Congress must eventually step in clarify the scope of Section 230 immunity, as we are currently trying to apply an innovative but outdated statute that has not kept up with our rapidly advancing technology.

I. BACKGROUND

A. The Early Internet

In the early 1990's, the internet looked a lot different than it does today. Rather than dropping its users into a vast, open world of information, the web was dominated by closed communities curated by internet companies.\textsuperscript{18} The major players in this universe were CompuServe, Prodigy, and America Online (AOL) and they all provided unique sets of information like “electronic versions of newspapers, newsletters, and financial advice.”\textsuperscript{19} There was no cross-platform operability during the internet's infancy. For example, an AOL subscriber could only see newsletters, posts, and articles provided by AOL users on AOL's platform and could not see

\begin{itemize}
\item \textsuperscript{16} See infra notes 198–203.
\item \textsuperscript{17} See infra Section III.C.1.
\item \textsuperscript{18} 26 WORDS, supra note 1, at 37.
\item \textsuperscript{19} Id.
\end{itemize}
This system of communication may sound restricted compared to the robust amount of information at our fingertips today, but at the time, users were being exposed to more information than any humans throughout history. Prior to the advent of the internet, Americans consumed nearly all their information through one-way channels like print or television media. These mediums were even more restricted than primitive cyberspace, hamstrung by the lack of user input and the inability to select what information was given to a user. The exciting new digital frontier opened the door to instant innovation, such as the creation of the online bulletin board, where users could post “special interest” information, research topics of interest, and “chat” by computer with another computer user live on the end of the line.

While this innovation marked the beginning of the age of information and would set humanity on the trajectory towards the tech-laden society we know today, there were growing pains. Indeed, the internet was like the wild west all over again. It was a blank canvas begging pioneers to leave their mark on its unadorned cyberscape. But across every ridge lied outlaws who, all-of-a-sudden, had unprecedented and near instantaneous access to millions of people across the country. These bad actors could log into their bulletin board of choice and post any number of lies, defamatory remarks, lewd photos or any other kind of unseemly information. Who were the police of this new frontier? The burden of policing fell on the companies like CompuServe and Prodigy who facilitated these forums. The merits of self-policing tech companies are a topic of debate even today, but the problems were worse back then. The lack of regulation caused firms to take drastically different approaches to regulating their platforms. On the one hand, companies like CompuServe decided to take a “hands-off approach” by not regulating user content at all. On

20. Id.
21. Id.
22. Id. at 38 (citing Martin Lasden, Of Bytes and Bulletin Boards, N.Y. TIMES (Aug. 4, 1985)).
23. Id.
25. 26 WORDS, supra note 1, at 38.
26. Id.
the other, companies like Prodigy "created and enforced user conduct standards." Prodigy even went as far as touting that it "[was] one of the few bulletin boards in the country to screen all electronic messages for potential improprieties." Unfortunately for Prodigy, no good deed goes unpunished. Its efforts to police its community by screening out tasteless content would expose it to infinitely more liability than it would have been exposed to had it done nothing at all.

Two cases would highlight this disconnect between law and policy and the national outrage that resulted would provide the basis for enacting Section 230. The first case, *Cubby, Inc. v. CompuServe, Inc.*, involved Bob Blanchard, an Emmy award-winning journalist. In 1990, Blanchard had launched the journalism industry rumor newsletter *Skuttlebut*. One of his competitors, Don Fitzpatrick, ran a similar newsletter titled *Rumorville*, which was based on CompuServe’s computer banks. In April 1990, *Rumorville* published a series of attacks on Blanchard. The attacks alleged that Blanchard had been fired from his previous employer—a New York ABC-affiliate television station—that Blanchard was the face behind *Skuttlebut*, and that Blanchard had been illegally accessing *Rumorville" through some [presumably illicit] back door." These statements were patently false and Blanchard sued both Fitzpatrick—under his businesses name Don Fitzpatrick Associates (“DFA”)—and CompuServe for libel, business disparagement, and unfair competition. This was the first lawsuit "on record that [sought] to hold an online service liable for a third party’s words."

CompuServe moved for summary judgement on all three claims and won. The distinction that gave rise to the dismissal was CompuServe’s lack of knowledge about what *Rumorville* had posted on its platform. Under the relevant libel laws, the defendant in a defamation suit must be found to be an original publisher or re-publisher of the defamation before they can be held liable. However,

---

27. Id.
28. Id. at 45.
30. 26 WORDS, supra note 1, at 38.
31. Id.
32. Id. at 38–39.
33. 26 WORDS, supra note 1, at 39.
35. 26 WORDS, supra note 1, at 39.
37. Id. at 141.
38. Id.
“vendors and distributors [like book stores and libraries]...are not liable if they neither know nor have reason to know of the defamation” that is contained in the products they distribute. Accordingly, CompuServe argued that, even though the Rumorville posts were doubtlessly defamatory, it could not be liable because it was “merely a passive distributor” of the content and was in no way a publisher of the defamation. CompuServe focused heavily on the facts that it had no direct relationship with Rumorville and did not review or edit the contents of Rumorville prior to its publication on the CompuServe platform. The district judge bought the defense, finding that there was no dispute of fact that (1) CompuServe exercised no editorial control over the defamation and was merely a distributor and (2) that CompuServe had no knowledge of the defamatory statements. Although this decision was probably correct under libel law, there is an inequitable result: CompuServe’s ability to avoid liability stemmed directly from its absolute refusal to moderate anything posted on its bulletin boards. Had it exercised any form of “editorial control” over the posts it facilitated, even if it made the internet a better place for the community, it likely would have been held liable.

Nowhere was this inequality more glaring than in a case that would follow a few years later. In Stratton Oakmont, Inc. v. Prodigy Servs. Co., Daniel Porush, the president of the infamous securities brokerage Stratton Oakmont, was the subject of a series of allegedly defamatory internet posts. The posts were made on Prodigy’s “Money Talk” forum in the wake of an initial public offering (“IPO”) of stock underwritten by Stratton. The IPO was for stock in Solomon-Page, “an employee recruitment company.” However, immediately after the IPO, Stratton and Solomon-Page “issued a prospectus revealing that Solomon-Page’s largest client, [UBS], was dropping” the firm. The posts hurled scathing allegations at Stratton Oakmont, claiming

39. *Id.* (citations omitted); see Smith v. California, 361 U.S. 147 (1959).
40. 26 WORDS, supra note 1, at 40.
44. Yes, *that* Stratton Oakmont—the Long Island securities firm founded by Jordan Belfort and depicted in Martin Scorsese’s *The Wolf of Wall Street*. In the film, Daniel Porush is portrayed by Jonah Hill who plays the right-hand-man to Leonardo DiCaprio’s Belfort. 26 WORDS, *supra* note 1, at 45.
45. 26 WORDS, *supra* note 1, at 45–46.
46. *Id.*
47. *Id.* at 45.
that the firm’s actions in underwriting the securities was “FRAUD, FRAUD, FRAUD” and that “STRATTON OAKMONT IS A CULT OF BROKERS WHO EITHER LIE FOR A LIVING OR THEY GET FIRED.”48 Weeks later, Porush filed a defamation suit against the John Doe defendants who made the posts and against Prodigy, seeking over $100 million in damages.49

Prodigy attempted to raise the same defense as CompuServe had in 1991 and claim that it was merely a distributor of the defamatory statements. Unfortunately for Prodigy, it had distinguished itself from CompuServe in the eyes of the court. In the “early 1990s, Prodigy aggressively promoted its family-friendly environment” and had a company policy to screen for obscenity, slander, and libel in content posted on its forums.50 Contracted Board Leaders for Prodigy had the ability to “delet[e] posts that failed to conform to the Prodigy guidelines.”51 Although Prodigy had long-since stopped manual editing of user posted content by October 1994, it still had an automated screening system designed to remove objectionable content.52 The Stratton Oakmont legal team seized on this distinction and argued that this made Prodigy a publisher of the defamation because it exercise “editorial control” of its board’s via its screening and removal procedures. The Nassau County trial judge agreed, finding that “By actively utilizing technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and ‘bad taste,’ for example, prodigy is clearly making decisions as to content... and such decisions constitute editorial control.”53

The result was alarming. How could the “good guy” of internet servers, the one who vowed to keep its communities safe from unseemly content, be the one that is held liable for its users’ actions? The implications had far-reaching consequences: If companies face legal liability for monitoring third-party content posted on their forums, they should stop monitoring content altogether, no matter how obscene, to ensure that they are not exposed to lawsuits.54

48. Id. at 46–47.
49. Id. at 48.
50. Id at 50.
51. Id.
52. Id. at 51.
53. Id. at 52 (citations omitted).
54. Id. at 55–56.
B. The Creation of Section 230

Though the Stratton Oakmont decision was a largely unheralded opinion from a New York state court, some members of Congress realized the potential harms done by the application of inadequate pre-internet common law to modern problems. Chris Cox, a California republican, and Ron Wyden, an Oregon democrat, decided to act. Both politicians had large constituencies in the tech industry as both of their congressional districts were proximate to Silicon Valley, Seattle, and Portland. Wyden recalled thinking “Why would anybody invest in a technology company if they thought they would be held personally liable?” However, one aspect of the internet that had not been overlooked by the rest of Congress was the growing amount of pornography and indecent content that was now accessible to children. To combat this epidemic, Senator James Exon introduced the Communications Decency Act of 1995, which, if enacted, would “prohibit the use of a telecommunications device[, such as an internet services company,] to knowingly make available ‘indecent’ material to minors under eighteen.” Cox and Wyden understood that, no matter the benevolent purpose of the proposed CDA, it existed as a threat to internet companies who would have “huge practical difficulties in complying with the bill.” Simply put, internet companies did not have the technology or the resources to comply with this demand, even though their failure to do so could result in hefty fines or imprisonment.

To counteract the negative effects on tech innovation, Cox and Wyden set out to create a new section of the Communications Act of 1934 that would accompany the Exon bill as an olive branch to the tech industry. The team had two express goals: (1) to encourage companies to develop online services without fear of liability and (2) to arm internet companies with the ability to regulate user content.
Due to the relatively small size of the internet at the time and the fact that most Congress people and the public at-large did not understand the internet very well, there was no significant opposition to the bill and its support in Congress received little media attention. The final conference committee wrote that the inclusion of Cox and Wyden’s Section 230 in the new bill had the express purpose of overruling Stratton Oakmont. On February 8, 1996, President Clinton signed the Telecommunications Act of 1996—including Section 230—into law.

The final version of the Cox and Wyden bill that was passed largely mirrors their goals and objectives at the onset of drafting the legislation. Section 230 is titled “Protection for private blocking and screening of offensive material.” Exemplifying the same sentiment for deregulation as Cox and Wyden, Congress adopted the findings that interactive computer services, like CompuServe and Prodigy, “offer a forum for a true diversity of political discourse [and...] myriad avenues for intellectual activity” and that these services “have flourished, to the benefit of all Americans, with a minimum of government regulation.” What’s more, Congress adopted the express policies of “promot[ing] the continued development of the Internet...and other interactive media” and “to preserve the vibrant and competitive free market that presently exists for the Internet.”

Section 230 has two operate provisions. Subsection (c)(1) states 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.” The term “interactive computer service” (“ICS”) is defined as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server...” including one that provides access to the internet.

---

63. Id. at 68–70.
64. Id. at 73; see also Brief of Senator Ron Wyden and Former Representative Christopher Cox as Amicus Curiae in Support of Respondent at 2, Gonzalez, v. Google LLC, No. 21-1333 (Jan. 19, 2023) 2023 WL 373840 [hereinafter Cox and Wyden Amicus Brief] (“Section 230 was in part a direct response to the New York Supreme Court’s decision in” Stratton Oakmont).
65. Id.
67. Id.
68. Id.
69. Id.
70. Id.
have interpreted it broadly to include websites, apps, and other forums.\textsuperscript{71} In plain English, this provision is understood as creating a liability shield for tech companies when users post defamatory statements on their platforms. The statute directly preempts the common law that created the inequities of \textit{Stratton Oakmont} by stating that internet service companies are not the “publisher or speaker” of content created by users.\textsuperscript{72} Rather, the company is treated as a distributor of the third-party content and is therefore not liable for any slander embedded in the content. On its face, this provision may seem rather innocuous. However, due to its brevity and a consortium of social, legal, and technological reasons discussed in this article, this provision has been one of the largest drivers of internet innovation.\textsuperscript{73} It is also mired in controversy and has been the subject of political animus for the last two decades.\textsuperscript{74}

The second provision protects computer services from liability if the company removes objectionable content from its forums—like what Prodigy had done.\textsuperscript{75} Subsection (c)(2) states that no ICS is liable for “any action [] taken in good faith to restrict access to ... material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.”\textsuperscript{76} This provision, though of approximately equal importance as (c)(1), packs more of a punch. Facialy, it gives ICSs and other tech companies the ability to broadly censor user speech, so long as they are acting in “good faith.”\textsuperscript{77} The law effectively balances the First Amendment rights to free speech and expression held by users with tech firms’ interest in moderating content and keeping our internet clean. Since its advent, “online platforms have adopted their own policies for user content and put in place innovative procedures and technologies to enforce these policies.”\textsuperscript{78} \textit{Have you ever wondered how Twitter can deplatform politicians, arguably violating their constitutional rights}

\textsuperscript{71} See 26 Words, supra note 1, at 65.
\textsuperscript{72} 47 U.S.C.A. § 230 (West).
\textsuperscript{73} 26 Words, supra note 1, at 9 (“Section 230 ‘has had enormous consequences for securing the vibrant culture of freedom of expression we have on the internet today.’” (citations omitted)).
\textsuperscript{74} See infra Section I.D.
\textsuperscript{75} 47 U.S.C.A. § 230 (West).
\textsuperscript{76} Id.
\textsuperscript{77} Id.
\textsuperscript{78} 26 Words, supra note 1, at 239.
in the process? Section 230(c)(2) is how. Indeed subsection (c)(2) has been one of the major drivers behind the empowerment of tech companies to moderate content on their platforms, and, much like its counterpart (c)(1), it has also been mired in controversy.\footnote{See infra Section I.D.}

C. Interpreting Section 230 and Its Modern Rules

1. Section 230’s Broad Liability Shield

Today, the majority of the platforms “that rely on user-generated content—such as Google, Facebook, Yelp, Wikipedia, and Twitter—are all based in the United States.”\footnote{26 WORDS, supra note 1, at 146.} No other western country could have facilitated this boom, as their laws are less friendly towards big tech.\footnote{Id. at 159 ("Other jurisdictions that generally share Western democratic values—such as Canada and Australia—have no equivalent of Section 230.").} “When [large tech] companies [are] starting out, they simply did not have the resources to litigate disputes over user content in Europe, Canada, and elsewhere.”\footnote{Id.; see Brief of Economists Ginger Zhe Jin et al. as Amicus Curiae in Support of Respondent at 3, Gonzalez v. Google LLC, No. 21-1333 (Jan. 19, 2023), 2023 WL 373841 [hereinafter Economists’ Amicus Brief] (“Websites could not exist as we know them today if they were liable for third-party content they disseminate.”).} Not all of this industry growth can be contributed to Section 230, but it’s hard to find a more formidable driver of tech-sector growth than the law that grants internet firms broad liability for their actions.\footnote{It is argued that this “success is at least partly attributable to Section 230 and the Digital Millennium Copyright Act.” Id. at 121.} In 2017, the Internet Association—a trade association comprised of leading internet companies—found that “of the twenty-one largest digital companies, thirteen are based in the United States.”\footnote{Id.} The greatest benefactor of this internet boom is America’s Silicon Valley, California.\footnote{VISIT SILICON VALLEY, https://visitsiliconvalley.org/explore-silicon-valley/ (last visited Mar. 16, 2023).} Today, 30 of the companies


\footnote{80. See infra Section I.D.}

\footnote{81. 26 WORDS, supra note 1, at 146.}

\footnote{82. Id. at 159 ("Other jurisdictions that generally share Western democratic values—such as Canada and Australia—have no equivalent of Section 230.".)}

\footnote{83. Id.; see Brief of Economists Ginger Zhe Jin et al. as Amicus Curiae in Support of Respondent at 3, Gonzalez v. Google LLC, No. 21-1333 (Jan. 19, 2023), 2023 WL 373841 [hereinafter Economists’ Amicus Brief] (“Websites could not exist as we know them today if they were liable for third-party content they disseminate.”).}

\footnote{84. It is argued that this “success is at least partly attributable to Section 230 and the Digital Millennium Copyright Act.” Id. at 121.}

\footnote{85. Id.}

\footnote{86. VISIT SILICON VALLEY, https://visitsiliconvalley.org/explore-silicon-valley/ (last visited Mar. 16, 2023).}
comprising the Fortune 1000 are located in the Valley,87 and there are over 40,000 different startups vying to take their place.88

So, how did we get here? How did one 26-word defamation liability shield and its content-moderation sibling help pilot America into the age of the internet? No case demonstrates the potential for this growth better than *Zeran v. America Online, Inc.*89 Zeran was the first case to interpret the scope and applicability of Section 230 after its enactment and the Zeran precedent would have a lasting effect on internet-era progress.90 In the wake of the bombings of the Alfred P. Murrah building in Oklahoma City, Kenneth Zeran began to receive angry calls and death threats.91 Zeran, a Seattle resident with no relation to the Oklahoma City bombing, was confused about the calls until he stumbled across an AOL post listing “Naughty Oklahoma T-Shirts” for sale and referencing him as the contact for purchase.92 That post disappeared, but, over the next few days, more posts would show up containing vile references to the bombings.93 The shirts for sale were adorned with slogans like: “Rack’em, Stack’em, and Pack’em—Oklahoma 1995”; “Shit happens. . . . to EXPLODE—Oklahoma 1995”; and “McVeigh for President 1996.”94 The angry calls continued to roll in and Zeran, who was understandably terrified, contacted AOL, the local police, and the FBI.95 During one of his many calls with AOL, he was reassured by company lawyer Jane Church that the posts would be removed.96 When the calls did not stop because AOL did not locate and eliminate the posts, Zeran sued AOL for negligence and failure to remove the harmful content.97

89. 129 F.3d 327 (4th Cir. 1997).
91. *Zeran*, 129 F.3d at 329.
92. *Id.*
93. 26 WORDS, *supra* note 1, at 80–81 (citations omitted).
94. *Id.*
95. *Zeran*, 129 F.3d at 329.
96. 26 WORDS, *supra* note 1, at 82 (citations removed).
97. *Id.* at 83 (citations omitted). The complaint was careful not to sue for defamation, and to sue for negligence instead because of the newly enacted Section
In the trial court, AOL moved for judgment on the pleadings relying solely on § 230 as its defense.98 This was a bold strategy by the AOL defense team, considering there was no case law to rely upon and the statute had been enacted primarily to apply to defamation claims—of which this was not.99 Essentially, under the newfound defense a defendant had to show that: (1) the posts were "information provided by another information content provider" (i.e. the jane Doe poster of the t-shirt ads) and (2) "that the suit treated the defendant as "the publisher or speaker" of the content.100 Luckily for thousands of future internet companies, the trial judge bought the defense, and created what would become the modern § 230 affirmative defense used by industry firms over the next 3 decades. Indeed, Judge Ellis wrote that "Zeran’s attempt to impose distributor liability on AOL is, in effect, an attempt to have AOL treated as the publisher" of the material and that "holding America Online liable for the anonymous postings would contradict Congress’s intent" in passing § 230.101

On appeal Zeran asked the Fourth circuit to overturn the decision and it declined to do so,102 adopting an exceptionally broad view of § 230 in the process. In its opinion, the court began by examining Congress’s intent in enacting § 230. It noted that Congress had made “a policy choice” that, although the “original culpable party” (the poster) would be held accountable for its actions, there was no “tort liability on companies that serve as intermediaries for other parties’ potentially injurious messages.”103 Judge Wilkinson also honed in on the statutory “purpose” delineated by Congress for enacting § 230: “preservation of the vibrant and competitive free market” of the internet and creating a “forum” for diverse political discourse, cultural development, and intellectual activity.104 The court next dispatched Zeran’s argument that, because § 230 only applies to “publisher liability” rather than “distributor liability,” it does not protect AOL.105 However, according to the court, these forms of liability were one-in-
the-same as distributor liability was a mere subset of publisher liability. Therefore, AOL must have the ability to raise the § 230 liability shield and, to do otherwise would have a “chilling effect on the freedom of internet speech.” The court also dismissed with Zeran’s clever pleading and noted that his choice to plead the action as negligence rather than defamation made no difference as the two are “indistinguishable.” Finally, the court explained that, if notice-based liability were imposed upon every computer service when they received a complaint about a post, “one angry person” could “censor online speech merely by lodging a complaint.” Then, these companies would have to conduct a thorough investigation followed by a judgment call on the removal of the post which, “in light of the vast amount of speech [on these services] could produce an impossible burden” for these companies.

Over the next few years, courts continued to follow judge Wilkinson’s lead and reaffirmed the broad interpretation of the § 230 defense. In Batzel v. Smith, Batzel hired Smith to handle some contractor work on her house. After a disagreement, Smith sent a false, inflammatory email about Batzel, a lawyer and art collector, to the Museum Security Network (“MSN”). He wrote that Batzel was the descendant of Heinrich Himmler and that hundreds of her extensive paintings on her wall were looted during World War II and that they rightfully belong to the Jewish people. The director of MSN, Mr. Cremers, edited the email, which contained Batzel’s contact information, and posted it on the MSN listserv and website. The fallout from the publication of the email caused Batzel to lose most of her business and effectively bankrupted her. Batzel sued Smith, Cremers, and the Netherlands Museum Association for libel, invasion of privacy, and intentional infliction of emotional distress.

Cremers—acting as MSN—moved to dismiss the case on § 230 grounds and, when the trial court refused, appealed to the Ninth

106. Id.
107. Id. at 333.
108. Id.
109. 26 WORDS, supra note 1, at 94.
110. Zeran, 129 F.3d 333.
111. 333 F.3d 1018 (9th Cir. 2003).
112. 26 WORDS, supra note 1, at 105.
113. Id.
114. Id. at 105–06.
115. Id.
116. Id. at 108.
Circuit. If ever there were a case to limit the scope of Section 230, it had to be this one, right? The defendant literally edited and posted the material himself on his online platform MSN. Wrong. The Ninth Circuit vacated and remanded the decision to deny the affirmative defense. Writing for the majority, Judge Berzon first stated her opinion that there was “no reason” for § 230 to exist and that First Amendment defamation law was more than sufficient to govern these matters. However, despite her suspicion, she held that it did not matter that Cremers had both distributed the email and made edits to it. According to the court “The ‘development of information’ means something more substantial than merely editing portions of an email” and publishing it. For this reason, Smith was the sole content provider of his defamatory email, and not Cremers. The implications of this decision are troubling even to the most ardent § 230 supporters. As Chris Cox, one of the two sponsors of Section 230, put it: “If that’s not a guy creating content, what the hell is that?”

Continuing the trend of broad § 230 immunity, two months later, the Ninth Circuit upheld the dismissal of numerous claims against Metrosplash, the corporate owner of Matchmaker.com, when a Matchmaker user created a defamatory profile depicting the actress Christianne Carafano. The profile at issue was characterized as “cruel and sadistic identity theft” and it included a picture of Carafano as well as sexually explicit answers to a questionnaire that was made by matchmaker and administered to its users. Although the questionnaire was curated by the platform and would help direct the user input that created the “content” at issue, there was not enough control for a finding of liability. Other decisions reinforced this broad interpretation of § 230 as well. In 2001 and 2002 alone, courts

---

117. Batzel, 333 F.3d 1018.
118. Id. at 1020.
119. Id. at 1031.
120. Id.
121. Id.
122. 26 WORDS, supra note 1, at 114.
123. Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003). Carafano is also known by her stage name “Chase Masterson,” and she has “appeared in numerous films and television shows, such as ‘Star Trek: Deep Space Nine,’ and ‘General Hospital.'” Id.
124. Id. at 1121.
125. Id. at 1124 (“Doubtless, the questionnaire facilitated the expression of information by individual users. However, the selection of the content was left exclusively to the user. The actual profile ‘information’ consisted of the particular options chosen and the additional essay answers provided.”).
issued written opinions in ten cases in which internet companies claimed § 230 immunity, and the defendant won eight times out of ten.\textsuperscript{126} Take, for example, Ripoff Report, a business review website that hosts user commentary on scams, bad reviews, lawsuits, and fraud.\textsuperscript{127} Largely due to Section 230 protections, Ripoff Report has spent more than $7 million in litigation and has not lost a single lawsuit.\textsuperscript{128} Indeed, much of the early history of Section 230 interpretation was dominated by tech-sector wins in courts throughout the country.\textsuperscript{129}

2. The Gradual Limiting of Section 230 Immunity

While early cases marked an expansive view of § 230 protections, later decisions have limited this powerful shield in small ways. As the social media and interactive app space expanded and more lawsuits around user-generated content arose, courts found exceptions to broad liability for internet intermediaries and crafty plaintiff’s lawyers exploited these exceptions. As Professor Kosseff explains in his book, there are two major ways to skirt section 230 immunity.\textsuperscript{130} One way to show liability for an internet company is to show that they were partly “responsible” for providing the content, since § 230 defines “information content provider” as one who is “responsible” for the creation or development of the content.\textsuperscript{131} This is what Carafano had unsuccessfully attempted to do by arguing that Matchmaker.com was “responsible” for creating the defamatory content because it gave a curated questionnaire to users that helped guide the user in creating their finalized postings.\textsuperscript{132} While Carafano ultimately failed, the Fair Housing Council of San Fernando Valley succeeded on a near identical theory years later.\textsuperscript{133} There, the court refused to dismiss

\begin{itemize}
\item \textsuperscript{126} 26 Words, supra note 1, at 203 (noting that “[t]he remaining two cases involved intellectual property claims, which are explicitly exempt from Section 230.”).
\item \textsuperscript{127} Id. at 122–24.
\item \textsuperscript{128} Id. at 126.
\item \textsuperscript{129} Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008) (immunizing Myspace under Section 230 for failing to take sufficient steps to prevent user-generated content by a sexual predator that led to the sexual assault of a 13-year-old girl).
\item \textsuperscript{130} 26 Words, supra note 1 at 165–70.
\item \textsuperscript{131} 47 U.S.C.A. § 230 (West); 26 Words, supra note 1, at 167.
\item \textsuperscript{132} See generally Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003).
\item \textsuperscript{133} Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1164 (9th Cir. 2008).
\end{itemize}
Rommates.com under § 230 when it had created questions and answers for user profile registration that indicated users’ sex, familial status, and sexual orientation. The Council alleged that this behavior was in violation of Federal Fair Housing standards because it prompted users to reveal information that could be used to discriminate against them. The court held that there is no immunity under § 230 for “inducing third parties to express illegal preferences” because the curated questions and answers were entirely the doing of Rommates.com. Judge Kozinski stated his opinion that § 230 “was not meant to create a lawless no-man’s land on the Internet” which, up to that point it history, it arguably had. Similarly, in Accusearch, the tenth circuit refused to immunize an internet company that connected its users to researchers, paid by the company, who would acquire confidential records on individuals that were protected by law. The court held that defendant Accusearch had “contributed mightily to the unlawful conduct of its researchers” and, therefore, was a content provider who was “responsible” for the illicit content.

The second way to get around the application of Section 230 is by “seeking to hold the website accountable for something other than publication or speech” of another party. One example is Doe v. Internet Brands, Inc. Internet Brands owned ModelMayhem.com which connected models with potential employers, and which it knew had been used to perpetrate “at least five previous sexual assaults” by one user. When a Jane Doe plaintiff was drugged and raped by the same perpetrator, she sued Internet Brands for their failure to warn her of the dangers of using ModelMayhem.com as a listing service. After Internet brands successfully sought immunity under § 230, the Ninth Circuit reversed the dismissal because the suit did not seek to hold Internet Brands for the publication or speech of the perpetrator

134. Id.
135. 42 U.S.C.A. § 3604(c) (West).
136. Rommates.com, 521 F.3d at 1165.
137. Id.
138. 26 WORDS, supra note 1, at 175.
139. F.T.C. v. Accusearch Inc., 570 F.3d 1187, 1200 (10th Cir. 2009).
140. 47 U.S.C.A. § 230 (West) (delineating that and interactive computer service shall not be “treated as the publisher or speaker” of third-party content); 26 WORDS, supra note 1, at 190.
141. Doe v. Internet Brands, Inc., 824 F.3d 846 (9th Cir. 2016).
142. 26 WORDS, supra note 1, at 196.
143. Id.
or another party.\textsuperscript{144} Rather, the suit sought to hold Internet Brands liable for \textit{its own speech} (or failure to speak) since it alleged the company had a duty to warn the plaintiff and did not.\textsuperscript{145} These decisions show that, although the Zeran holding remains intact, courts may be skeptical about the extent of § 230 immunity.\textsuperscript{146} As a result, the 230 immunity shield remains strong, but it is no longer impenetrable.

D. Section 230 and Its Dissenters

Section 230 has been integral to the rapid expansion of the American tech industry and is a large driver for the progress that produced the technology-laden society we know today.\textsuperscript{147} However, this rapid progress has also produced detractors who question the continued need for this broad liability shield and who disapprove of the broad protections afforded to social media companies, internet platforms, and industry conglomerates. The most ardent of these dissenters are members of the republican party. On multiple occasions, Justice Clarence Thomas has admonished the body of law interpreting § 230(c)(1) immunity, stating: “Many courts have construed the law broadly to confer sweeping immunity on some of the largest companies in the world.”\textsuperscript{148} In his eyes, courts have placed too much importance on the “polic[ies] and purpose[s]” of Congress in enacting § 230 and have read “extra immunity” into the law “where it does not belong.”\textsuperscript{149} In March of this year, conservative leadership held the 2023 Conservative Political Action Conference (CPAC) which hosted a panel titled “Big Tech – Break ‘em Up, Bust ‘em Up, Put ‘em in jail.”\textsuperscript{150} On the panel was Florida attorney general Ashley Moody

\textsuperscript{144}. Id. at 198.
\textsuperscript{145}. Id.
\textsuperscript{146}. Id. at 199 (quoting Judge Clifton in his \textit{Internet brands} opinion as stating “Congress has not provided an all purpose get-out-of-jail-free card for businesses that publish user content on the internet, though any claims might have a marginal chilling effect on internet publishing businesses).
\textsuperscript{147}. See supra notes 81–88.
\textsuperscript{148}. Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13 (2020).
\textsuperscript{149}. Id. at 15.
who characterized § 230 as allowing internet platforms to “publish information and not be held liable” for it.\textsuperscript{151}

Also drawing the ire of the republican party is §§ (c)(2), the lesser-litigated but equally potent provision immunizing tech companies who censor and remove content.\textsuperscript{152} In the wake of the January 6th assault on the U.S. Capitol building, Twitter took the unprecedented step of permanently banning a U.S. President from its platform when it Banned Donald Trump.\textsuperscript{153} President Trump repeatedly utilized social media to get his messages to his constituents, and Twitter had, on numerous occasions, censored his tweets or tagged them with a note that they may contain “misinformation.”\textsuperscript{154} Twitter was empowered to do all of this through § 230(c)(2)’s protections. Following these and other steps by big tech to sensor conservative speech, Florida\textsuperscript{155} and Texas\textsuperscript{156} both passed legislation forbidding social media companies from, amongst other things, censoring user speech, deplatforming users based on viewpoints, and deplatforming politicians. Additionally, these statutes contain requirements such as public disclosure of content moderation guidelines,\textsuperscript{157} a complaint and appeal system for content removal,\textsuperscript{158} and user ability to opt-in or out of “shadow banning” algorithms.\textsuperscript{159} The Florida law was struck down by the 11th Circuit in NetChoice, LLC v. Att’y Gen., Fla.\textsuperscript{160} while the Texas law was upheld by the 5th Circuit in NetChoice, L.L.C. v. Paxton.\textsuperscript{161} Conservatives, however, aren’t the only ones who’ve expressed distaste in the application of § 230. President Joe Biden has shared the sentiment that Section 230 should be “revoked” immediately.\textsuperscript{162}

\begin{itemize}
\item \textsuperscript{151} Id.
\item \textsuperscript{152} See 47 U.S.C.A. § 230(c)(2) (West).
\item \textsuperscript{153} Danny Crichton, The Deplatforming of President Trump, TECHCRUNCH.COM (Jan. 9, 2021) https://techcrunch.com/2021/01/09/the-deplatforming-of-a-president/.
\item \textsuperscript{154} Id.
\item \textsuperscript{155} See FLA. STAT. ANN. § 106.072 (West); FLA. STAT. ANN. § 501.2041 (West).
\item \textsuperscript{156} See TEX. BUS. & COM. CODE ANN. § 120.001 et seq. (West).
\item \textsuperscript{157} TEX. BUS. & COM. CODE ANN. § 120.051 (West).
\item \textsuperscript{158} TEX. BUS. & COM. CODE ANN. § 120.101 et seq. (West).
\item \textsuperscript{159} FLA. STAT. ANN. § 501.2041 (West).
\item \textsuperscript{160} 34 F.4th 1196 (11th Cir. 2022).
\item \textsuperscript{161} 49 F.4th 439, 445 (5th Cir. 2022).
\end{itemize}
Outside of the political sphere, there is plenty of discussion around the inequitable results of Section 230 immunity. One group whose interests seem most at odds with Section 230 are women. This is largely because “the victims of the most vile online harassment campaigns are often women” who may be attacked through revenge porn, defamatory posts, or cases of identity theft. These are women like Christianne Carafano who had a fake, sexually-explicit parody account of her posted on Matchmaker, leading to multiple instances of harassment. Or the 13-year-old Jane Doe plaintiff who was the victim of predatory posts on Myspace that led to her rape. Or Cecilia Barnes, whose ex-boyfriend posted nude photos of her and her contact information on yahoo, resulting in a deluge of vulgar phone calls from strangers. Indeed, due to their vulnerabilities, the cases of women seeking redress for harmful activity that occurred on the internet are legion. Even judges are skeptical of the breadth of Section 230 immunity. Judge Berzon, whose controversial decision to immunize Tom Cremers when he edited and posted a defamatory email about Ellen Batzel, expressed her doubts about the statute. Before issuing her opinion absolving Cremers and MSN of liability, she stated:

There is no reason inherent in the technological features of cyberspace why First Amendment and defamation law should apply differently in cyberspace than in the brick and mortar world. Congress, however, has chosen for policy reasons to immunize from liability for defamatory or obscene speech

---

163. 26 Words, supra note 1, at 222.
164. See supra notes 106–08.
166. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1097 (9th Cir. 2009), as amended (Sept. 28, 2009) (holding that Barnes was not able to advance her negligence claim against Yahoo for failing to remove the posts after promising to do so, but that Barnes could advance her promissory estoppel claim on the same theory).
167. See e.g., Jones v. Dirty World Ent. Recordings LLC, 755 F.3d 398, 401 (6th Cir. 2014) (holding that a gossip website was immunized under § 230 after it facilitated defamatory posts referring to a Bengals cheerleader that contained false details about her sex life and STD testing results even though the editor added his own commentary at the end of the post).
168. See e.g., supra note 129 (noting, in the opinion immunizing Myspace in the Doe case, that Section 230 was not intended to be an “all purpose get-out-of-jail-free card”).
169. See supra notes 117–122.
“providers and users of interactive computer services” when the defamatory or obscene material is “provided” by someone else.\textsuperscript{170}

Indeed, “there is a rising chorus of judicial voices cautioning against an overbroad reading of the scope of Section 230 immunity.”\textsuperscript{171} Much of this caution stems from the rapid advancement of screening technology and the fact that “websites are leveraging new technologies to detect, flag, and remove large volumes of” unseemly content.\textsuperscript{172} In the eyes of judges, this new technology has taken away much of the burden associated with content moderation and the process is more effective and less onerous for platforms.\textsuperscript{173} Therefore, in their opinion, Congress should reduce the immunity provided by \textsection 230 in this new world where content moderation is relatively easy.\textsuperscript{174}

Unfortunately for these politicians, victims of online harassment, and judges assigned to \textsection 230 cases, there is a wide body of law dating back to \textit{Zeran} that goes against their arguments.\textsuperscript{175} This body of law has driven internet-era progress and the American economy for decades, while also growing ever more controversial with each decision. At some point, the high court will need to make a decision: \textit{Do we, as a country, continue to immunize tech platforms at the expense of users when they are harmed by having their speech stifled or suffer online harassment? Or do we abolish the liability shield that has contributed mightily to the world we know today?} This controversial decision could be made in the coming months.

\textbf{II. Section 230 Gets Its Day in Court: Gonzalez v. Google}

On November 9, 2015, Jordanian police Captain Anwar Abu Zaid smuggled in an AK-47 to work, and opened fire on the International

\textsuperscript{170} Batzel v. Smith, 333 F.3d 1018, 1020 (9th Cir. 2003).
\textsuperscript{171} Gonzalez v. Google LLC, 2 F.4th 871, 896 (9th Cir. 2021), cert. granted, 214 L. Ed. 2d 12, 143 S. Ct. 80 (2022), and cert. granted sub nom. Twitter, Inc. v. Taamneh, 214 L. Ed. 2d 12, 143 S. Ct. 81 (2022).
\textsuperscript{172} Id. at 896–97.
\textsuperscript{173} Id. at 897.
\textsuperscript{174} Id.
\textsuperscript{175} Id. (“In sum, though we agree the Internet has grown into a sophisticated and powerful global engine the drafters of \textsection 230 could not have foreseen, the decision we reach is dictated by the fact that we are not writing on a blank slate. Congress affirmatively immunized interactive computer service providers that publish the speech or content of others.”).
Police Training Center in southeast Amman. Following the attack, the terrorist group Islamic State of Iraq and Syria (“ISIS”) took credit for the murders, boasting that “we kill the Americans In Amman.” Fields and Creach’s widows sued Twitter for violating the Anti-Terrorism Act (“ATA”) alleging that Twitter had provided “material support” to ISIS by knowingly and recklessly supplying it with Twitter accounts which led to the deaths of the Americans. A direct connection between Abu Zaid, Twitter, and ISIS was never confirmed and there were no concrete facts establishing that Abu Zaid carried out his attacks as a result of ISIS activity on Twitter. However, up until 2014, Twitter utilized a “largely hands-off approach to terrorist” and other objectionable content, claiming that, in the interests of preserving first amendment rights, you had “to take the good with the bad.” This allowed ISIS to create an estimated 70,000 Twitter accounts and to promote many of its jihadist killings on the platform.

Twitter moved to dismiss the lawsuit on Section 230 immunity, as well as other grounds, claiming that “[n]ot even the thinnest of reeds connects Twitter to this terrible event.” After multiple amended complaints and subsequent motions to dismiss, the trial court agreed with Twitter stating that “[n]o amount of careful pleading can change the fact that, in substance, plaintiffs aim to hold Twitter liable as a publisher or speaker of ISIS’s hateful rhetoric, and that such liability is barred by the CDA.” Plaintiffs appealed to the Ninth Circuit who affirmed the dismissal on other grounds and never reached a conclusion on whether Section 230 immunized Twitter. In the eyes

177. Id.
178. Id.
180. Fields, 881 F.3d at 742.
181. 26 WORDS, supra note 1, at 230–31.
182. Id. at 231.
183. Fields, 881 F.3d at 742.
184. 26 WORDS, supra note 1, at 231 (demonstrating how ISIS had promoted its killing of a Jordanian pilot Maaz al-Kassabeh on Twitter).
185. Id.
186. Id. at 243.
187. Fields, 881 F.3d at 750.
of the court, the lack of connection between Twitter’s “hands off” approach and the harm suffered by Fields and Creach was significant, and that the plaintiffs had not successfully plead proximate causation of the harm.\(^{188}\)

This case was the first of its kind that sought to hold a tech platform liable for terrorist content posted on its site.\(^{189}\) However, the Northern District of California opinion immunizing Twitter under Section 230 is still good law and numerous other district and appellate courts have come to the same conclusion in similar cases.\(^{190}\) Victims of terrorism were not mentioned above in the groups of Section 230 dissenters, but, much like women, they are among the groups most frequently litigating its broad liability shield. Indeed, terrorists are often directly or indirectly motivated by propaganda posted on social media sites and it is possible to imagine a scenario where a social media site could potentially be liable for hosting that propaganda.\(^{191}\)

Earlier this year, the Supreme Court granted certiorari in two companion cases seeking to hold giant tech conglomerates liable for hosting terrorist speech that led to loss of American lives.\(^{192}\) The decisions to be handed down will be the first time that the Supreme Court will address the issue of Section 230 protections for companies hosting terrorist speech. More importantly, however, this will also be the first time that the Supreme Court has ever interpreted the broad liability shield at all.

The first case stems from a “series of attacks perpetrated by ISIS in Paris” on November 13, 2015 (the “Paris Attacks”).\(^{193}\) Nohemi Gonzalez, a 23-year-old American studying abroad in Paris, was massacred when three ISIS members opened fire on the café where she was enjoying dinner with her friends.\(^{194}\) ISIS executed several brutal bombings and shootings throughout the French capital and the group took to YouTube to claim responsibility for the crimes the following day.\(^{195}\) Nohemi’s father, Reynaldo Gonzalez, brought suit against YouTube via its parent company Google, seeking to hold Google liable under the ATA for directly and secondarily committing

\(^{188}\) Id.

\(^{189}\) 26 WORDS, supra note 1, at 236.

\(^{190}\) Id.; see Force v. Facebook, Inc., 934 F.3d 53, 57 (2d Cir. 2019) (immunizing Facebook from liability under the ATA for attacks carried out by the terrorist organization Hamas).

\(^{191}\) Id. at 237.

\(^{192}\) See Gonzalez, 2 F.4th 871.

\(^{193}\) Id. at 880.

\(^{194}\) Id.

\(^{195}\) Id. at 880–81.
acts of international terrorism. The complaint claimed that YouTube “has become an essential and integral part of ISIS’s program of terrorism” since two of the twelve Paris attackers posted links to “jihadi YouTube videos” and the organization utilized YouTube frequently in its recruiting efforts.

The complaint made two specific allegations. First, that Google utilized its recommendation algorithms—used to match users with preferential content on YouTube—to “[recommend] ISIS videos to users’ and enabled users to ‘locate other videos and accounts related to ISIS.’” An algorithm “is simply a set of digital instructions to recognize certain patterns about users and, based on those instructions, filter information most pertinent to users.” Algorithms are decidedly prevalent in our digital world and most major internet platforms use algorithms in some capacity—such as Google, Twitter, Yelp, Bing, and Facebook. This reliance on mathematical equations exists because “the internet is host to far more content than any human could review, sift, or benefit from without the aid of sorting mechanisms.” Algorithms are now a “crucial feature of the modern economy” and they are how platforms, politicians, businesses, and people sift through the “120 zettabytes of data online.” Through these algorithms, Gonzalez alleged, Google was “assist[ing] ISIS in spreading its message.”

Second, the complaint alleged that YouTube shared revenue with ISIS through its video monetization process, since YouTube approved ISIS videos for monetization and placed ads on those videos that would generate revenue for the benefit of ISIS. The trial court found “that all of Plaintiffs’ claims were barred by § 230” except the

196. Id.
197. Id.
198. Id.
200. Id.
201. Id.
203. See Gonzalez, 2 F.4th at 881.
204. Id.
205. Id. at 882–83. Some of the claims were also found to have not alleged sufficient proximate causation of the harm suffered to the victims. Id.
revenue sharing claims that were eventually abandoned by the plaintiffs.206

The second case was borne out of the 2017 Reina nightclub massacre in Istanbul, Turkey.207 Early in the morning on New Year's day, Abdulkadir Masharipov—an ISIS affiliate—walked into Reina nightclub and "fired more than 120 rounds into the crowd of 700 people, killing 39 and injuring 69 others."208 The following day, "ISIS issued a statement claiming responsibility for the Reina Attack."209 Among the 39 dead was Nawras Alassaf, who was bringing in the New Year with his wife at the bar that fateful morning.210 His relatives brought suit, alleging—much like the Gonzalez family did—"that Google, Twitter, and Facebook were a critical part of ISIS's growth."211 The complaint stated that the three companies were directly liable under the ATA for providing material support to ISIS and secondarily liable aiding and abetting ISIS activities by allowing them to utilize their platforms.212 Unlike the Gonzalez case, the trial court did not dismiss the action on § 230 grounds. Instead, the court held that the "direct liability claims failed to adequately allege proximate cause [and] the secondary liability claims failed to state a claim" for conspiracy or for aiding and abetting under the ATA.213

The dismissed cases came before the Ninth Circuit as a consolidated action.214 However, since the trial court in Taamneh did not rule on Section 230 grounds, the ninth Circuit did not apply Section 230 law to Taamneh facts215 and the plaintiffs are not asking the Supreme Court to do so either.216 As a result, this case is less important to our Section 230 inquiry and this paper will almost exclusively focus on the issues presented in the Gonzalez case.

On appeal, Reynaldo Gonzalez asserted two categories of arguments related to Section 230: (1) that § 230 didn’t apply to his

207. Id. at 883.
208. Id.
209. Id.
210. Id.
211. Id.
212. Id. at 884.
213. Id.
214. Id.
215. Id. at 907–08.
216. Brief for Petitioner at 1, Twitter, Inc., v. Taamneh, No. 21-1496 (Nov. 29, 2023), 2022 WL 17384573 (stating that the questions presented resolve issues of the ATA and JASTA—Justice Against Sponsors of Terrorism Act—rather than § 230).
claims against Google at all, and (2) that, even if it did, his claims survived the application of § 230. His claims that § 230 doesn’t apply to these facts were as follows: “(1) § 230 immunity has no application to extraterritorial claims; (2) Congress impliedly repealed § 230 when it amended the ATA in 2016; and (3) § 230 immunity does not apply to ATA claims based on criminal statutes.”

The court dispatched with each of these quickly finding: (1) that the regulated conduct—civil litigation involving internet companies—occurred entirely in the U.S., (2) the ATA did not impliedly repeal § 230 as the two are not at odds in any way, and (3) that § 230 does clearly apply to “civil actions based on criminal statutes,” of which this is.

The Ninth Circuit then turned to the modern three elements of the § 230 defense that was born out all the way back in Zeran. It reiterated: “Section 230(c)(1) precludes liability for “(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat ... as a publisher or speaker (3) of information provided by another information content provider.” If all of these elements are demonstrated, then the defendant is immune to the action. As for the first factor, the parties were not in dispute that Google is an “interactive computer service.” The term is interpreted rather expansively and certainly includes the world’s largest search engine. Second, the court found that the nexus of the complaint “is that Google did not do enough to block or remove content, and that such claims necessarily require the court to treat Google as a publisher.” The court explained that “[p]ublishing encompasses ‘any activity that can be boiled down to deciding whether to exclude material that third parties seek to post online...’” Here, the complaint was succinctly stating that YouTube failed to remove ISIS content and was therefore engaging in publisher activities.

The third element of the defense was more contentious and gets to the heart of the issue: Do YouTube’s algorithms “create” or “develop”

217. Gonzalez, 2 F.4th at 886.
218. Id.
219. Id. at 888.
220. Id. at 889.
221. Id. at 890.
222. Id. (citations omitted).
223. Id.
224. Id. at 891.
225. Id.
226. Id. at 892 (citing Roommates, 521 F.3d at 1170–71).
“the content that appears on a users’ feed, thereby making YouTube itself the creator of the content?” Remember how one way to plead around Section 230 immunity is to show that the defendant was somehow “responsible” for the creation or development of the content itself? This is that same exact argument. Much like Christianne Carafano and the Fair Housing Council of San Fernando Valley had done in their cases, Reynaldo Gonzalez had to paint Google as the “creator” or “developer” of the harmful ISIS videos. Unfortunately for the plaintiff, the argument fell flat due to the application of what’s known as the Ninth’s Circuit’s “material contribution” and “neutral tools” tests. Under this jurisprudence, a “material contribution” [to third-party content] does not refer to “merely augmenting the content generally, but to materially contributing to its alleged unlawfulness.” Taking action to display the content is not sufficient, the defendant must “be[] responsible for what makes the displayed content allegedly unlawful.” As a sub-rule to the “material contribution” doctrine, the “neutral tools” test holds that “[a] website does not create or develop content when it merely provides a neutral means by which third parties can post information of their own independent choosing online.”

The application of these tests led to the ultimate undoing of the plaintiffs’ case because the circuit had already determined that the neutral tools test immunized algorithms uses by internet companies. In Dyroff, the mother of a message board user sued the website when her son purchased heroin after making an inquiry on about drugs on the message board. The court held that section § 230 immunized the message board when it used algorithms to “analyze” and “recommend” user content because the “neutral” algorithms were “not content in and of themselves.” Therefore, the company as not liable when its algorithms provided a third-party answer describing

227. Id.
228. See supra Section I.C.
229. Gonzalez, 2 F.4th at 892. (“The Gonzalez Plaintiffs are correct that § 230 immunity only applies to the extent interactive computer service providers do not also provide the challenged information content.” (citing Roommates, 521 F.3d at 1162–63; Carafano, 339 F.3d at 1123)).
230. Id. (citing Roommates, 521 F.3d at 1167–68 (emphasis added)).
231. Id.
232. Id. at 893 (citations omitted).
233. Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093 (9th Cir. 2019).
234. Id. at 894.
235. Id.
Applying these standards, the Ninth Circuit in *Gonzalez* held that YouTube’s recommendation algorithms were in no way distinguishable from the ones in *Dyroff* or even the matchmaking process in *Carafano*.237 The court reasoned that all of the algorithms at issue were based on user inputs and the tools merely matched those inputs with historical viewing actions to make recommendations based on what the user may like.238 The algorithms in no way targeted ISIS content for promotion “or designed its website to encourage videos that further the terrorist group’s mission.”239 The court finally noted that the Second Circuit—in *Force*—came to the exact same conclusion when applying § 230 to claims under the ATA that Facebook’s algorithms created terrorist content.240 There, the Second Circuit held “that Facebook’s algorithms may have made content more visible or available, but [that] this did not amount to developing the underlying information.”241 Ultimately, Reynaldo Gonzalez could not overcome these precedents.

It must be noted, however, that neither the *Force* decision nor the *Gonzalez* decision was unanimous. In *Gonzales*, Judge Gould partially dissented from the majority’s application of § 230 immunity to Google, relying in-part on “Chief Judge Katzmann’s cogent and well-reasoned opinion” in *Force*.242 There Judge Katzmann disagreed with the notion that Facebook’s algorithms were immune from liability under § 230 for two reasons. “First . . . that Facebook’s algorithms communicated their own message—i.e., the algorithms suggested the user would likely be interested in certain additional content . . . [and s]econd, Facebook’s friend—and content—suggestion algorithms created and maintained ‘real-world social networks.”’243 According to Katzmann, Facebook’s algorithms did more than play the role of mere publisher, they were communicating their own messages that persuaded users to join a “unique global community.”244 Indeed, Facebook “collects detailed information about its users including[] the content they post, type of content they view or engage with, people they communicate with, groups they belong to and” other data before utilizing that

236. *Id.*

237. *Id.*

238. *Id.* at 895.

239. *Id.*

240. *Id.* (citing *Force*, 934 F.3d at 64–72).

241. *Id.*

242. *Id.* at 920 (Gould, J., dissenting).

243. *Id.* at 896.

244. *Force*, 934 F.3d at 82 (Katzmann J., dissenting).
information to “suggest friends, groups, products, services and local events, and target ads” to users. For Katzmann, this clearly made Facebook the speaker of its own content via its algorithms. Judge Gould largely adopted Katzmann’s application of § 230 as applied to YouTube. In his view, when YouTube “automatically” queues a new video for a user without the user prompting the app to do so, the algorithm making the recommendation is not acting as a “neutral tool.” Instead, Judge Gould would have held that § 230 does not immunize Google’s conduct “to the extent that it amplified and in part developed the terrorist message by encouraging” susceptible users to view similar ISIS videos.

After the Ninth Circuit’s decision, Mr. Gonzalez appealed to the Supreme Court who granted certiorari on October 3rd, 2022. In their brief, petitioners asked the court to address a broad, open-ended question of § 230 application: “Under what circumstances does the defense created by section 230(c)(1) apply to recommendations of third-party content?” The question tracks the same issues raised in the Ninth Circuit’s opinion when it sought to determine if YouTube was “responsible” for the recommendations that its algorithms made. Petitioners assert that immunity “is not available for material that [a] website itself created”—such as an algorithm’s recommendation. Google’s defense is largely the same as well. It asserted that it had “no role whatsoever in ‘creating’ or ‘developing’ alleged ISIS videos” and that the three elements needed to raise the § 230 defense are met.

However broad the petitioner’s proffered question may be, the ramifications of this decision are certainly much broader. Implicitly, the petitioners are asking the court: when, if ever, are tech companies

245. Id. (Katzmann J., dissenting).
246. Id. (Katzmann J., dissenting).
247. Gonzalez, 2 F.4th at 920 (Gould, J., dissenting).
248. Id. at 921–24 (Gould, J., dissenting).
249. Id. at 922 (Gould, J., dissenting).
251. Microsoft Amicus Brief, supra note 19, at 6. This question was much broader than the original question proposed in their petition.
immune under § 230 when their algorithms recommend third-party content? As mentioned above, algorithms are a “crucial feature” of the modern economy and we depend on them for almost everything we do involving the internet.254 “Targeted recommendations are now ubiquitous across the Internet” and online functionality would largely cease to exist as we know it without algorithms.255 “Simply put, the stakes could not be higher.”256

On February 21st, the Supreme Court held oral arguments on this issue.257 The Justices posed questions and offered hypotheticals and opinions that helped us garner insight into what they may be thinking. The remainder of this article, and really the crux of my argument, will be analyzing (1) what the court may decide, (2) the fallout from that decision, and (3) any potential solutions that the court, individual actors, and society as a whole may enact to limit exposure to any unwanted ramifications of this decision.

III. POTENTIAL OUTCOMES IN GONZALEZ AND THE RESULTING Fallout

A. The Nuances of the Gonzalez Case: Attenuated Causation, Stale Facts, and an Aging Bench

Before addressing the potential ramifications of the court’s decision, there are some important nuances that I must note. For starters, it’s not immediately clear why the Supreme Court is even hearing these cases. Sure, Section 230 is the source of much political controversy.258 And yes, few—if any—statutory laws have had such a broad impact on our daily lives.259 Accordingly, it seems logical that the high court would want to leave its mark on the law and attempt to resolve some of the surrounding controversy. However, this case is missing some of the hallmarks of cases where the court would traditionally grant cert. For example, there is no circuit split. In fact, the two circuits who have directly addressed the issue of Section 230 to internet algorithms have come to the exact same conclusion:

254. Id. at 10.
255. Cox and Wyden Amicus Brief, supra note 48, at 12.
256. Microsoft Amicus Brief, supra note 199, at 4.
258. See supra Section I.D.
259. See supra note 81–88.
companies are immunized for the algorithm recommendations.\footnote{260} What’s more, since the opinion in \textit{Zeran}, federal courts across the country have stuck to a consistently-broad interpretation of Section 230 for decades, deviating only under limited circumstances.\footnote{261} Accordingly, without a definitive legal controversy to resolve, it leaves us to wonder if the court is engaging in activism and is attempting to prematurely resolve the political controversy.

Adding to this perplexity is the fact that the causation between YouTube recommendations and ISIS conduct is attenuated to say the least. In \textit{Gonzalez}, the trial court found that a large chunk of the plaintiffs’ claims “failed to plausibly allege Google proximately caused the Gonzalez Plaintiffs’ injury.”\footnote{262} As Google noted in its brief:

> Petitioners did not allege that any Paris attacker saw any ISIS videos based on this feature or, indeed, that YouTube played any role in bringing about the Paris attack. Instead, the complaint contained one screenshot taken a year after the attack purporting to “show[] a video that was recommended based upon other videos [a user] had viewed in the past”... The complaint did not specify what those previous videos entailed or what the recommended videos showed.\footnote{263}

Much like in \textit{Fields} and other cases involving terrorism and social media, the facts showing causation and proximate causation are incredibly hard to discover and prove.\footnote{264} Much of this may be due to the international location of the perpetrators and the lack of documentation regarding what all they may have watched or read that influenced their decisions.

Not only are the facts attenuated with regard to causation, but they’re also a little bit stale. “YouTube’s terms prohibit ISIS and other terrorist groups from using YouTube, and YouTube has repeatedly blocked ISIS accounts.”\footnote{265} Since 2016—nearly a year after the facts in \textit{Gonzalez}—YouTube has taken dozens of steps to help screen and

\begin{doublespace}
\footnotesize
\begin{itemize}
\item 260. See Force, 934 F.3d 53 (immunizing algorithms under Second Circuit jurisprudence); Dyroff, 934 F.3d 1093 (immunizing algorithms under Ninth Circuit jurisprudence).
\item 261. See supra Section I.C.
\item 262. Gonzalez, 2 F.4th at 882–83.
\item 263. Respondent Brief, supra note 202, at 15.
\item 264. See source cited supra note 181.
\item 265. Respondent Brief, supra note 202, at 14.
\end{itemize}
\end{doublespace}
remove offensive conduct from its platforms.\textsuperscript{266} These steps include augmenting machine learning with human flagging to detect harmful or terrorist content.\textsuperscript{267} Additionally, Google and other internet companies and governments founded the Global Internet Forum to Counter Terrorism ("GIFCT") in direct response to the epidemic of terrorists utilizing social media for their operations.\textsuperscript{268} The Forum maintains a broad "hash-sharing" database containing known images representing terrorist content that have been posted to internet platforms.\textsuperscript{269} The hash is a "numerical representation of original [terrorist] content" that is added to the database so that other forum members can "can quickly identify if the same content is shared on their platform and assess it in line with their policies and terms of service."\textsuperscript{270} This push for better moderation of terrorist content goes well-beyond Google and extends industry-wide.\textsuperscript{271}

Congress and legislative bodies are also doing their part as well, challenging tech executives "about their efforts to keep ISIS and other groups off their platforms."\textsuperscript{272} While not perfect, these measures have had an effect to the extent that, now, groups like the Islamic State must find new ways to work around detection procedures, such as: encrypting text, scrambling images, and using broken text.\textsuperscript{273} Despite these efforts, YouTube is able to take down content in about 30 minutes, although some of its tech-sector counterparts are not nearly as effective.\textsuperscript{274} This will always be a sort of cat-and-mouse game amongst terrorists and the platforms or websites they attempt to exploit. Eradicating terrorist content from the internet altogether is

\textsuperscript{266} The YouTube Team, \textit{The Four Rs of Responsibility, Part 1: Removing harmful Content}, \textsc{YouTube Official Blog} (Sep. 03, 2019), https://blog.youtube/inside-youtube/the-four-rs-of-responsibility-remove/.

\textsuperscript{267} Id.


\textsuperscript{269} GIFCT’s Hash-Sharing Database, GIFCT.ORG, https://gifct.org/hsdb/.

\textsuperscript{270} Id.

\textsuperscript{271} Id.

\textsuperscript{272} 26 WORDS, supra note 1, at 237 (noting that the hearing was titled “Terrorism and Social media: #IsBigTechDoingEnough?”).


\textsuperscript{274} Id.
impossible at the moment. However, thanks to GIFCT and industry-wide efforts, the internet today is a far cry from the “hands-off,” anything-goes internet that existed at the time of the facts in Gonzalez.275

Finally, I would be remiss if I didn’t note that, historically, the Supreme Court is awful at understanding modern technology and is not the best body to interpret laws regarding it. Members of the bench have admitted themselves that “they’re not the most technologically sophisticated people.”276 Many of them have scarcely even come into contact with the technologies they are asked to adjudicate over.277 After all, the majority of them are in their 60’s and 70’s and would have had a limited grasp on modern technology that was not around in their developmental years.278 Accordingly, issues regarding modern tech—especially convoluted ones like algorithms that hardly anyone outside of the industry fully understands—are better regulated by a younger, more knowledgeable body.

For these reasons alone, determining why the court chose these two cases as its first crack at Section 230 is perplexing. There is no circuit split, the facts are 8 years old and do not reflect modern developments in counter-terrorism technology, and the court is certain to struggle grasping the concept of algorithms with any proficiency. However, whatever motivations may exist, their decision is certain to impact our lives in a meaningful way.

B. What We Know About the Justices Individually and Cumulatively

Before determining how the court may go forward with their decision and the ramifications of any potential decisions, it is

275. See supra notes 265–71.
276. Greg Stohr, Social Media Case Test Limits of Supreme Court’s Tech Savvy (2), BLOOMBERG LAW (Feb. 14, 2023), https://www.bloomberglaw.com/bloomberglawnews/exp/eyJjdHh0IjoiQVOVyIsImlkIjoiMDAwMDAxODYrNTA4OS1kMDI1LWtjYWJtNWNmOTZiNi02UEU2MDAxODAyNTkwIiwic21nIjoiaSkxZG9nY25rYSIsImVkaXJpdGlvbkNsaWNrIjoiWkM0bGd3ZlB6ZjAxMDM1IiwicGF0ZmluaXR1cmVCIjoiY2FsbGlnaHRsZSIsInByb2ZpbGwiOiJQV191QUNvZ2h0Iiwic3R5bGUiOiJ0ZWFyeS1tb251bGwsIiwiZXhwIjoiZjJjODM5ZGI2MDI2MSwiZW1vdWxkZXJzIjoiaHR0cHM6Ly9hdXNvZ3NhdGljZC5jb20vQ2FudGVyL1ZlcnNpb25zL29taXVzb3VyY2UsMTY5ODI4MjA5MzQ1Ljg2NzAyIiwidGltZHMiOiJzdHlsZSIsImNvbnZlcnQiOjEwIiwicm9vdF9lbWJlZCI6IjBFTU9TQ2FudGVyIiwic3R5bGUiOiJ0ZWFyeS1tb251bGwsIiwiY2xvd2lsbF9pZCJdLCJzZW5kXCI6IiJ9. 277. Id. (recounting the story of Justice Breyer playing Grand Theft Auto in his office to get a better understanding of violent video games and noting that he characterized the game as “disgusting and repellant”).
important to briefly address valuable insights that were gleaned
during oral arguments in the Gonzalez case. Below are some of the
insights about the Justices’ potential stances on the matter.

1. Justice Clarence Thomas

As is noted above, Justice Thomas is openly critical towards
Section 230.279 In his opinion, courts have interpreted Section 230 too
broadly and have chosen to immunize tech companies in a way that
Congress did not intend.280 However, despite this being somewhat of
a republican party-line stance on the matter, Justice Thomas is the
only Justice currently on the bench who has given us much insight
into his feelings prior to oral arguments.

Interestingly, whatever criticism he may harbor toward the law
itself, he did not seem particularly interested in using this case to
upend it. As a general theme of his questioning, he seemed fixated on
the notion that the Ninth Circuit’s application of the “neutral tools”
test was correct.281 Regarding YouTube’s recommendation of ISIS
videos to those who frequently watch content of that nature, he stated
to petitioners’ counsel: “And I don’t understand how a neutral
suggestion about something that you’ve expressed an interest in is
aiding and abetting. I just don’t --I don’t understand it.”282 It appears
from his comments that, so long as an application is “using the same
algorithm across the board,” it should not be liable for its algorithmic
recommendation of third-party content.283 Accordingly, although
Justice Thomas is the Justice who should be viewed as most likely to
limit Section 230 immunity, he does not necessarily appear ready to
do so in this case.

2. Justice Neil Gorsuch

Justice Gorsuch appears likely to take the opposite stance from
Justice Thomas, as his comments implied, at the very least, that he
doesn’t agree with the Ninth Circuit’s “neutral tools” test. In a
hypothetical proffered to petitioners’ counsel, Justice Gorsuch
proposed that “in a post-algorithm world” artificial intelligence and
other advanced technologies could generate content in the form of

279. See supra notes 148–49.
280. See supra notes 148–49.
282. Id.
283. Id. at 5.
recommendations, that goes beyond picking and choosing content—which are the traditionally-protected editorial actions under Section 230. According to Justice Gorsuch, the court had three options: (1) find for Google, (2) find for petitioner, or (3) remand the case to the Ninth Circuit because the “Neutral Tools test was mistaken [as], in some circumstances, even neutral tools, like algorithms, can generate through artificial intelligence forms of content and that the Ninth Circuit wasn't sensitive to that possibility.” Justice Gorsuch later characterized some of the flaws found in the “neutral tools” assessment:

And another problem also is that it begs the question what a neutral rule is. Is an algorithm always neutral? Don't many of them seek to profit-maximize or promote their own products? Some might even prefer one point of view over another. And because the Ninth Circuit applied the wrong test, this neutral tools test, rather than the content test, we should remand the case for reconsideration under the appropriate standard. Is that a fair summary of your position?

As a result, it appears that, while Gorsuch may not wish to find for petitioners at this time, he is questioning the application of the neutral rules test to the facts of this case and the legality of the standard as a whole. This would likely result in a remand, were he to write for the majority.

3. Chief Justice John Roberts and Justices Amy Coney Barrett and Brett Kavanaugh

Being two of the youngest Justices on the Court, Justices Barrett and Kavanaugh appear to share the same concerns: broadened liability as a ramification of limiting Section 230. Justice Kavanaugh explicitly expressed apprehension that, if the Court found for petitioner, the statute would essentially “defeat itself.” He explained that, if algorithm recommendations voided liability for internet platforms, “the very thing that makes the website an interactive computer service also mean[s] that it loses the protection

284. Id. at 49.
285. Id. at 50.
286. Id. at 101.
287. Id. at 52.
of 230." He then grilled petitioners' counsel on the "economic dislocation" that would result were the court to stray away from its broad liability shield jurisprudence. Similarly, Justice Barrett expressed concerns that, if the petitioners' reading of Section 230 was adopted, social media users could be potentially liable for "retweeting" or "liking" terrorist content because they would then be creating content in the same manner that an algorithm does. She was even able to get petitioners' counsel to agree with her concerns. Though never explicitly stated, this contention was obviously at odds with public policy since allowing lawsuits against all users who retweet potentially harmful content would be a dubious proposition.

Chief Justice Roberts shared in these concerns and noted his agreement with multiple amici about the potential for frivolous litigation if they limit Section 230 immunity. He stated:

We're talking about the prospect of significant liability in litigation, and up to this point, people have focused on the ATA because that's the one point that's at issue here. But I suspect there would be many, many times more defamation suits, discrimination suits, as -- as some of the discussion has been this morning, infliction of emotional distress, antitrust actions.

Overall, these three seemed most amicable towards keeping the broad § 230 liability shield that has been in place for decades, at least for now.

4. Justices Ketanji Brown Jackson and Elena Kagan

Arguably the two most hostile Justices—at least in their questioning—towards Section 230 were Justices Jackson and Kagan. While addressing respondent's counsel, Justice Jackson explicitly proposed the idea that Section 230 had been interpreted too broadly. She stated:

[I]sn't there something different to what Congress was trying to do with 230? Isn't it true that that statute had

288. Id.
289. Id. at 54–57.
290. Id. at 59–62.
291. Id.
292. Id. at 85–86.
 Moreover, she directly opposed the notion that Congress wanted to bootstrap the success of the internet with its passing of Section 230, despite clear evidence to the contrary. In the same vein, Justice Kagan noted her disquiet in applying a “pre-algorithm” statute to a “post-algorithm world.” She also challenged the notion that tech companies and the internet are exceptional by nature and proposed that, maybe, they don’t actually deserve any special treatment. She stated to petitioners’ counsel:

I can imagine a world where you’re right that none of [these algorithms and recommendations] gets protection. And, you know, every other industry has to internalize the costs of its conduct. Why is it that the tech industry gets a pass? A little bit unclear.

According to Justice Kagan, tech firms should potentially be responsible for internalizing the cost of litigation over their recommendations because, even if there would be a flood of meritless litigation against the platforms that are now essentially our public forums, other sectors must internalize their costs as well. Overall, and somewhat unexpectedly, two of the more liberal Justices on the bench appeared as the most hostile towards Section 230.

5. General Confusion on the Bench

One recurrent theme throughout the oral arguments was the lack of understanding by the Justices about both the technology and the
arguments at issue. A major source of confusion was the inability to draw a clearly defined line in petitioners’ argument. Early on, petitioners’ counsel argued that thumbnails on YouTube videos are YouTube’s own content and, therefore, are not immunized by Section 230. Justice Alito and Justice Jackson both expressed an inability to delineate when third party content (ISIS’s own videos) becomes YouTube’s content (a thumbnail recommendation containing ISIS’s own video). Justice Sotomayor recognized that having a line between third-party conduct (posting a video) and platform conduct (YouTube’s recommendation of that video) “seems logical.” However, the court was “suffering” with this distinction and had clearly been looking hopelessly for that line throughout the argument. It was not clear before the close of petitioners’ arguments that this line was ever effectively drawn.

At other points, the age and technological incompetence of the Justices were on full display. Well after his initial “line-drawing” series of questions about the thumbnails, Justice Alito was still “completely confused by whatever argument [petitioners were] making at the [] time.” This confusion was reaffirmed multiple times by other justices, such as Justice Jackson—“I guess I’m thoroughly confused” by petitioners arguments—and Justice Thomas—“Well, I’m still confused.” Justice Kagan was well aware of the uncertainty that tainted the bench, and she quipped: “I mean, we’re a court. We really don’t know about these things. You know, these are not like the nine greatest experts on the Internet. (Laughter [from the gallery].)” Indeed, the entire transcript is laden with a distinct lack of understanding about how to parse out these highly-technical and complicated arguments. This is not entirely the Courts’ fault as some of it is due to subject matter. Even more
technologically-competent, younger laypeople who grew up with this technology at their fingertips, would struggle to follow the more nuanced points of argument. In sum, the court did not seem to have a strong grasp on the technology at issue and, as is demonstrated below, this will likely benefit Google in the end.310

6. A Hesitancy to Engage in Activism

No matter how bad their political counterparts may want them to,311 many Justices on the bench did not appear eager to engage in judicial activism. After expressing the idea that the tech-sector might should take responsibility and internalize the costs of this litigation, Justice Kagan exhibited hesitancy that this was the court’s decision to make.312 Instead, she noted that this may be “something for Congress to do, not the Court[].”313 Justice Kavanaugh shared the same sentiment, stating “isn't it better for [us] to put the burden on Congress to [rewrite Section 230 so that] they can consider the implications and make these predictive judgments?”314 This hesitancy towards altering the status quo has been a constant in Section 230 litigation. Even judges who are highly critical of Section 230 immunity and its oft-inequitable outcomes have explicitly stated their preference that Congress do the heavy lifting on this issue.315 Indeed, many judges are aware that there is a body of law on the matter that has been developed over decades and it started with a Congressional action that it thought was in the best interest of Americans at the time.316 Much like others who have been asked to interpret Section 230 immunity, members of the Court did not seem particularly interested in undoing what Congress had set in motion.

310. See infra Section III.C.1.
311. See supra Section I.D.
312. See Gonzalez Oral Argument, supra note 206, at 46.
313. Id.
314. Id. at 82.
315. See Force, 934 F.3d at 77 (Katzmann, J., dissenting) (“Congress may wish to revisit the CDA to better calibrate the circumstances where such immunization is appropriate and inappropriate in light of congressional purposes.”).
316. Gonzalez 2 F.4th at 897 (“In sum, though we agree the Internet has grown into a sophisticated and powerful global engine the drafters of § 230 could not have foreseen, the decision we reach is dictated by the fact that we are not writing on a blank slate. Congress affirmatively immunized interactive computer service providers that publish the speech or content of others.”).
C. Potential Outcomes in Gonzalez and the Resulting Fallout

1. The Court Guts or Limits Section 230 Immunity: The Truman Show Versus a Horror Show

The first possible outcome in the Gonzalez case is that the court limits, or even guts, the broad § 230 immunity shield that has existed since Zeran. This outcome is more than theoretical, it’s entirely plausible. As Professor Kosseff notes, under an expansive reading of the Ninth’s circuit’s jurisprudence in Roommates.com and Accusearch, a social media site could conceivably be held as “responsible for the ‘development’ of illegal content” based off the recommendations of its algorithms.317 Moreover, “[a]s platforms increasingly develop more sophisticated algorithm-based technology to process user data” this scenario may become more likely.318 Justice Gorsuch admitted as much at oral arguments when he urged Google’s counsel to agree that, at least “in the abstract,” the application of the “neutral tools” test to YouTube’s algorithms could produce a scenario where Section 230 does not immunize Google.319 If the Court were to go this route, it is not immediately clear what the main holding would be. However, we know from the facts of the case that the YouTube algorithms were “neutral” in nature which appears to be standard throughout the tech industry.320 Accordingly, any holding that limits Section 230 immunity for these algorithms is likely to apply to every other algorithm, since they appear facially indistinguishable.

This is the doomsday scenario. It would be hard to imagine a decision that could be more disruptive to an industry than cutting away the “building block” on which it was founded.321 As has been covered, algorithms and recommendations are “crucial” to essentially every modern internet platform, website, and app.322 The internet cannot function in the same way as it currently does without the use of algorithms and mathematical sorting tools that make decisions in place of humans.323 Accordingly, the logical conclusion of this holding is that internet companies are liable for everything hosted on their

317. 26 WORDS, supra note 1, at 188–89.
318. Id.
319. See Gonzalez Oral Argument, supra note 206, at 151–53.
320. See Gonzalez, 2 F.4th 871 (holding that Google was immunized by the “neutral tools” test due to the neutral application of its algorithms to ISIS content).
platforms because, at some point, *every piece of content they host is recommended* by an algorithm. The results would be dystopian.\(^\text{324}\) Indeed, companies would be faced with two potential choices: (1) remove any and all content that could even be considered objectionable for fear of liability if it is recommended, or (2) moderate and recommend absolutely nothing, for fear that the recommendations and moderations are actionable.\(^\text{325}\) One of these two outcomes is almost certain to occur in every applicable case. Essentially, you have what amounts to “[T]he Truman Show versus a horror show” where either (1) only highly-filtered “happy talk” is allowed on the internet, or (2) uncensored filth and “garbage” flood the digital space.\(^\text{326}\)

The first untenable result of limiting Section 230 immunity is the over-correction by the industry that results in extreme moderation. Although this scenario would have an equally horrible effect on all of us, I have chosen to dub this the “conservative prisoner’s dilemma” because of the conservative stance on the issue. The republican party is doubtlessly the most vocally critical demographic of Section 230 protections.\(^\text{327}\) Generally speaking, they believe the law has given “Big Tech” too much power and has been interpreted by courts do give immunity to parties who Congress never intended to immunize.\(^\text{328}\) As a group, they are often the ones who are most effected by content moderation\(^\text{329}\) and they believe there is a “biased silencing” of their first amendment rights “as conservatives ... by the ‘big tech oligarchs in Silicon Valley.’”\(^\text{330}\)

Unfortunately for conservatives—and truly for everyone—the very statute that they abhor may be what protects their first amendment rights the most. “In a world where websites are pressured to preemptively remove third-party content that might trigger litigation, websites would be even more leery of permitting political (including conservative-leaning) speech on hot-button topics.”\(^\text{331}\) In this world, many tech firms who do not want the exposure to liability would immediately and unequivocally remove any content that could conceivably be actionable.\(^\text{332}\) If a company wants to avoid being sued

\(^{324}\) Respondent Brief, *supra* note 202, at 5.

\(^{325}\) *Id.*

\(^{326}\) *See Gonzalez Oral Argument, supra* note 206, at 125.

\(^{327}\) *See supra* text accompanying notes 147–51.

\(^{328}\) *See supra* text accompanying notes 147–51.

\(^{329}\) *See supra* text accompanying notes 147–51.

\(^{330}\) *Att’y Gen., Fla.,* 34 F.4th 1196.

\(^{331}\) Respondent Brief, *supra* note 202, at 53.

\(^{332}\) *Id.*
for hosting objectionable content, the simplest way to do that is to throw anyone who may say anything objectionable off the platform preemptively.

David Sacks is a lawyer, venture capitalist, podcaster, and conservative commentator who has a unique perspective on this case due to his legal background, conservative views, and decades of experience in the tech industry. On his podcast hosted with other venture capitalists, he noted his fears that the conservative majority on the Court is “gonna make the same mistake that conservative media has been making” by “dramatically...limit[ing] Section 230” protection. This, he argues, will “blow up in our collective faces.”

According to him, “if you repeal Section 230” believing it will lead to less conservative censorship, you are going to, instead, get “vastly more censorship” for everyone due to “simple corporate risk aversion.”

The very reason internet platforms remain “open” at all is because they have “distributor” liability under Section 230, and they cannot be sued as a “publisher” of content. Without this distinction, they have no incentives to allow controversial speech.

Economists agree. Writing as amici, economists from some of the nation’s leading universities note that strict censorship is inevitable in this scenario and that “[l]awful but controversial expression would be especially vulnerable.” Some may go as far as “allowing only known, trusted actors to create content.” More importantly, the fallout would have a disproportionate impact on the startup ecosystem in America. The greater risk of liability would make it harder for start-ups to get off the ground at all because they have little “capacity to survive even meritless lawsuits.” In America, our unique system of laws—headlined by Section 230—has created a startup ecosystem where the greatest tech companies in the world have thrived. Without this legal incubator, it is likely that Google, Facebook, Yelp, Wikipedia, Twitter and other titans could not have existed, as “they simply did not have the resources to litigate disputes

---

333. All-In with Chamath, Jason, Sacks & Friedberg, E116: Toxic Out-of-Control Trains, Regulators, and AI, at 39:10 (downloaded using Spotify).
334. Id.
335. Id.
336. Id.
337. Economists’ Amicus Brief, supra note 83, at 4.
338. Id.
339. Id.
340. Id.
341. See supra text accompanying note 81–88.
over user content in Europe, Canada, and elsewhere.\textsuperscript{342} Litigation—especially complex corporate litigation—is expensive and legal fees may potentially “exceed a startup’s valuation.”\textsuperscript{343} Moreover, startups are ill equipped to hire sufficient compliance staff that would be needed to comply with new regulatory body that would develop after Section 230’s repeal.\textsuperscript{344} The end result is that, not only are startups hamstrung with legal and compliance costs, they may also receive less funding from risk-averse, skittish investors.\textsuperscript{345} Investors do not want to fund ventures that run the risk of being sued into oblivion, and “a United States company protected by Section 230 is ‘5 times as likely to secure investment over $10 million and nearly 10 times as likely to receive investments over $100 million, as compared to internet companies in the [European Union].’”\textsuperscript{346} Accordingly, the impact could be drastic, going as far as eliminating the ecosystem that was built to harbor the next generation of Facebooks, Googles, and Twitters.

The Second untenable scenario is much more direct and its ramifications are easily discernable: internet companies would refuse to regulate, recommend, and moderate anything. This is the very harm that Congress intended to prevent when it enacted Section 230. Congress’s stated purpose in passing Section 230 was to remedy the inequalities between Cubby—where CompuServe was absolved of liability because it refused to moderate user content at all—and Stratton Oakmond—where Prodigy was held liable because it tried to create a family-friendly online environment through content moderation.\textsuperscript{347} Indeed those companies who do not go the route of excessive moderation would be forced to “shut[] their eyes” to objectionable content, as tech companies were incentivized to do by Cubby and Stratton Oakmond.\textsuperscript{348} The end result is an undoing of progress and a “race to a bottom of pornography or other offensive material—the 1990s phenomenon that prompted Section 230 in the first place.”\textsuperscript{349}

Thankfully, this hellscapae of over-and-under-moderation seems unlikely for four reasons. First, as is mentioned above, both the Court and other judges who have reviewed Section 230 issues do not seem

\begin{itemize}
  \item \textsuperscript{342} 26 WORDS, supra note 1, at 147.
  \item \textsuperscript{343} Economists’ Amicus Brief, supra note 83, at 11 (citations omitted).
  \item \textsuperscript{344} Id.
  \item \textsuperscript{345} Id. at 11–12.
  \item \textsuperscript{346} Id.
  \item \textsuperscript{347} See supra Section I.A.
  \item \textsuperscript{348} Respondent Brief, supra note 202, at 5.
  \item \textsuperscript{349} Id. at 54.
\end{itemize}
inclined towards activism. It is true that conservatives harbor the most vitriol towards the law and it is also true that the majority currently on the bench is conservative-leaning. However, multiple Justices expressed the sentiment that, if someone were going to significantly alter Section 230 immunity, it should be Congress who does it. Accordingly, it seems likely that the court would rather not act to change the broad immunity shield currently in place, unless their hand was forced by the right case or Congressional inaction. Second, the Court may also be too confused by the Gonzalez issues to limit Section 230. At points, Justices Alito, Jackson, Thomas, Sotomayor, and Kagan all expressed confusion about either the arguments made by petitioners, algorithmic technology, or both. One would think that the stale, complicated, and attenuated facts causing this confusion would force the court to believe that this is not the right case to go about re-writing laws.

Third, the conservatives—who are presumed as the most likely to strike down Section 230—did not appear hostile towards the law during oral arguments. Chief Justice John Roberts and Justices Amy Coney Barrett and Brett Kavanaugh, overall, acted most favorably towards keeping broad Section 230 immunity. Even Justice Thomas, who we know thinks Section 230 has been interpreted too broadly, was not overtly hostile during oral arguments. Finally, although the sentiment was not universal, multiple members of the court seemed keenly aware of the hellish consequences that would befall technology innovation if Section 230 were limited. Chief Justice Roberts expressly adopted the view that there would potentially be “many, many times more” lawsuits against tech firms that would lead to over-and-under-regulation. Similarly, Justice Kavanaugh refuted petitioners’ claims that the potential litigation frenzy “would not be that bad” because most of the claims would not be actionable. Rather, he seemed to recognize that “[t]here will be lots of lawsuits”—both defamatory and otherwise.

In sum, limiting Section 230 immunity is the worst-case scenario. The result would be “[T]he Truman Show versus a horror show” on
internet platforms, where companies are forced to over-moderate everything or to do nothing at all. Startups would be the most impacted, and the ramifications could potentially be felt years down the road when companies are less likely to be founded in a space where they may be subject to endless litigation. Thankfully, the court does not seem particularly inclined to go this route, and we should hope that they don’t change their minds.

2. The Court Upholds Broad Section 230 Immunity

Simply put, this would maintain the status quo of federal Section 230 jurisprudence. As a result, not much analysis is required here. The most logical method of upholding Section 230 immunity would be to expressly adopt the Ninth Circuit’s “neutral tools” test, and to uphold the Circuits’ application of the “neutral tools” test to Google. This can be boiled down to a three-step process. First, the court would need to adopt the “material contribution” framework announced in Accusearch, ruling that an internet company does not “create” or “develop” third party content unless it makes a “material contribution” to the content at issue. Second, the court would expressly adopt the “neutral tools” test, holding that “[a] ‘website does not create or develop content when it merely provides a neutral means by which third parties can post information of their own independent choosing online.’” Finally, the court would need to expressly rule that algorithms—ones that apply equally regardless of content type as Google’s do—are “neutral tools” under the jurisprudence and that platforms are, therefore, immunized for recommendations made by their algorithms. This decision would bind the circuit courts to this framework, and would unite the other circuits with the Second Circuit’s decision in Force and the Ninth Circuit’s decision in Gonzalez.

There would be little to no immediate resulting fallout if the court goes this route. They would merely be adopting the decades of jurisprudence that has established broad Section 230 immunity in the lower courts. The only major changes would be that (1) any other circuit who hears a Section 230 case on algorithms must apply the “neutral tools” rule and (2) Supreme Court precedent would enshrine

358. See Gonzalez Oral Argument, supra note 206, at 125.
359. See supra text accompanying notes 230–32.
360. See supra text accompanying notes 230–32.
361. See supra text accompanying note 232.
362. See supra Part III.
363. See supra Section I.C.
broad immunity into law and would make it harder to limit the doctrine later—at least in theory. While this option is certainly better than the nuclear option above, as I will show below, a maintenance of the status quo may merely be a stopgap before Section 230 is eventually overhauled.\footnote{364. See infra Section III.D.}

3. Remand: The Court May “Kick the Can Down the Road”

The Court may choose to buck the “neutral tools” framework and establish their own test for Section 230 immunity as applied to algorithms. However, I do not wish to go down the rabbit hole of speculation on various ways they could uphold immunity without adopting the “neutral tools” rule. That could take dozens of pages. Moreover, since two of the circuits have already expressly adopted the “neutral tools” rule, it seems most likely that this is an all-or-nothing proposition: the court will either adopt the rule or strike it down. Still, at oral arguments, at least one Justice—Justice Gorsuch—seemed keen on remanding with instructions to eliminate or modify the “neutral tools” test.\footnote{365. See Gonzalez Oral Argument, supra note 206, at 50.} He stated that the Court could find for Google, find against Google, or “could say the Ninth Circuit’s Neutral Tools test was mistaken because, in some circumstances, even neutral tools, like algorithms, can generate through artificial intelligence forms of content and that the Ninth Circuit wasn’t sensitive to that possibility and remand the case for it to consider that question.”\footnote{366. Id.} He pressed petitioners’ counsel who reluctantly admitted this was “a correct analysis” of the Court’s options.\footnote{367. Id. at 51.} Later, he pressed respondent’s counsel by espousing all of the flaws he found in the “neutral tools” framework.\footnote{368. Id. at 151.} He stated:

I guess my problem with [the neutral tools test] is that language isn’t anywhere in the statute, number one. Number two, you can use algorithms as well as persons to generate content, so just because it’s an algorithm doesn’t mean it [can’t generate content], it seems to me. And third, that I’m not even sure any algorithm really is neutral. I’m not even sure what [the neutral tools] test means because most algorithms are designed

\footnote{364. See infra Section III.D.}
these days to maximize profits... So I -- I guess I'm not sure I understand why the Ninth Circuit's test was the appropriate one and why a remand wouldn't be appropriate... 369

His argument has some merit. Just because an algorithm is neutral in its recommendation doesn't mean it isn't creating content. An "up next" recommendation, even one that's neutral, is still implicitly conveying the message that the user should watch a certain video because (1) they will like it and (2) it will make YouTube money. 370 Still, by that same rationale, nearly anything—recommendations, suggestions, removing people from platforms, search-engine optimization, basic sorting, etc.—would convey a message. Adopting this rationale would lead us to the same result as finding for petitioners: companies would be scared to engage in content moderation at all. 371

Regardless of the merits of the arguments, if Justice Gorsuch were to persuade a majority of the Court to decide this way, he would merely be delaying the inevitable. Irrespective of who won or lost on remand, at some point, the court will need to rule on Section 230 as applied to algorithms and potentially more broadly. This leads me to my final argument that, even if the Court steers us clear from the dystopian results of limiting Section 230, either Congress, the Court, or both will have more work to do.

D. The Gonzalez Decision Will Not Resolve the Dispute Over Section 230: Moody and Paxton

If Section 230(c)(1) is the great shield wielded by social media companies, Section 230(c)(2) is the sword that completes their armor. Indeed, subsection (c)(2) is what empowers social media platforms and other tech firms to censor, moderate, and deplatform users who violate their terms of conduct. 372 Feeling as though their First Amendment rights had been violated "by the 'big tech' oligarchs in Silicon Valley" wielding §§ (c)(2)'s power, politicians in Florida and

369. Id. at 151–152.
370. See Id. at 22–25 (explaining petitioners' rationale that "next up" recommendations in YouTube go beyond the activities of an interactive computer service and make YouTube a publisher for giving users content that they did not ask for).
371. See supra Section III.C.1.
372. See supra text accompanying notes 75–80.
Texas decided to take a stand.\footnote{Att’y Gen., Fla., 34 F.4th at 1205 (citations omitted).} After the online censorship of former President Donald Trump\footnote{See supra text accompanying notes 152–62.} and others, Ron DeSantis—now Trump’s biggest political opponent—pushed Florida S.B. 7072 through the state legislature to put an end to the “biased silencing” of conservatives.\footnote{Att’y Gen., Fla., 34 F.4th at 1205 (citations omitted).} The bill, signed into law in 2021, mandates that “social media platforms,” amongst other requirements, (1) cannot deplatform a Florida political candidate for more than 14 days, (2) cannot “shadow ban” journalists or users posting political commentary, (3) must allow users to opt-out of prioritization algorithms, (4) must publish content moderation rules and (5) must thoroughly explain every act of “censorship of users.”\footnote{Id. at 1205–07.} Essentially, the law directly pushes back on Section 230(c)(2)’s grant of authority for social media platforms to censor user content at will.\footnote{Subsection (c)(2) states that no ICS is liable for “any action [] taken in good faith to restrict access to ... material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.” 47 U.S.C.A. § 230 (West).}

Around the same time, Texas passed HB 20 seeking to regulate “platforms with more than 50 million monthly active users . . . such as Facebook, Twitter, and YouTube.”\footnote{Paxton, 49 F.4th at 445 (citations omitted).} Similar to the Florida bill, HB 20 made it (1) illegal for platforms to censor anyone based on their viewpoints or location in Texas and (2) mandated that platforms maintain an “acceptable use policy,” a “biannual transparency report,” and a “complaint-and-appeal system.”\footnote{Paxton, 49 F.4th at 445-46 (citations omitted).} Both laws were challenged separately in federal district courts by NetChoice, a trade association that represents large social media companies.\footnote{Att’y Gen., Fla., 34 F.4th at 1207 (citations omitted).} NetChoice sought to enjoin enforcement of both the Florida\footnote{Id. at 1207 (citations omitted).} and Texas\footnote{Paxton, 49 F.4th at 447 (citations omitted).} laws on grounds that they are unconstitutional. The Western District of Texas found that all of the challenged provisions of HB 20 were facially unconstitutional and that they fail any level of heightened scrutiny as they “chill the social media platforms’ speech.”\footnote{Id. at 1207 (citations omitted).} Similarly, the Northern District of Florida held that S.B. 7072 came “nowhere close”
to passing strict First Amendment scrutiny because there was no
government interest in passing the bill other than to burden social
media companies.384 Both district courts granted injunctions to
NetChoice.385

On appeal, however, the Eleventh and Fifth circuits split,
adopting holdings that directly opposed one another and causing a
significant issue of federal law in the process. In the Florida case, the
Eleventh Circuit first held that social media companies' content
moderation activities are "editorial judgments" that are protected by
First Amendment jurisprudence.386 In doing so, the court shot down
the idea that social media companies are modern-day "common
carriers" who possess little or no First Amendment rights merely
because they act as a public forum and provide a necessary service.387
Both Supreme Court precedent and Congressional act distinguish
social media companies from common carriers.388 Next, the court held
that—with one exception—all of the Florida law's mandates on social
media platforms restricted their editorial judgements and triggered
First Amendment scrutiny.389 The court then bifurcated S.B. 7072's
requirements into two groups: those that restrict content-moderation
(like bans on censorship) and those that require disclosure (like the
publication of platform rules).390 Finally, the court held that all of the
content-moderation restrictions failed to "survive intermediate—let
alone strict—scrutiny" because they failed to advance any substantial
governmental interest, much less any compelling one.391 On the other
hand, most of the disclosure provisions fared much better and were
likely to be found constitutional.392

Conversely, the Fifth Circuit came to a completely opposite
conclusion, finding that First Amendment scrutiny did not apply to
the Texas law at all.393 Instead, HB 20 "protects other people's speech
and regulates the Platforms' conduct."394 The court explained that,
under Supreme Court precedent, NetChoice "must show that the
challenged law either (a) compels the host to speak or (b) restricts the

385. Id.; Paxton, 49 F.4th at 447.
386. Att'y Gen., Fla., 34 F.4th 1210 (citations omitted).
387. Id. at 1219–20.
388. Id. at 1202–21.
389. Id. at 1222.
390. Id. at 1226–27.
391. Id. at 1227–28.
392. Id.
394. Id. at 448.
host’s own speech.”395 Here, NetChoice could do neither because censorship is not considered speech, according to the Fifth Circuit.396

Finally, the court also adopted the application of the common carrier doctrine to social media companies—in direct contrast with the Eleventh Circuit—because the platforms are members of the communications industry who “hold themselves out to serve the public.”397 As a result, social media companies would be entitled to little or no First Amendment protections, due to their common carrier status.398

Both Ashley Moody—the Florida Attorney general who lost in the Eleventh Circuit—and NetChoice—who lost in the Fifth Circuit—petitioned the court for a writ of certiorari.399 The question presented to the court in both cases can generally be stated as: (1) whether the First Amendment applies to state laws regulating social media platforms’ authority to moderate content and, (2) if so, do any of the regulations in the Texas and Florida laws pass First Amendment scrutiny.400 The Supreme Court has not yet granted cert in either case and it is not immediately clear if they are going to do so at all. However, if they do, this may be the more likely vehicle by which the Supreme Court will start to eat away at Section 230’s powers for a few reasons.

First, although the issues presented pertain to First Amendment protections and the lower courts did not focus on Section 230 issues, these statutes are in direct conflict with Section 230(c)(2)’s grant of power for tech companies to regulate “objectionable” user content as they see fit.401 If the Court upholds the provisions in these laws, they are effectively allowing states to write over Section 230’s grant of power, if they wish to do so. Second, the Court should take the case, as there is a ripe, justiciable issue to resolve in the form of a circuit split. Unlike in Gonzalez, there is not a body of caselaw dating back decades that has resulted in multiple lower courts interpreting the

395. Id. at 459.
396. Id.
397. Id. at 473–74.
398. Id.
issue the same.402 Instead, this is a rather novel issue regarding modern, unique laws and the circuits interpreting those laws have come to wildly different conclusions about their legality. As a result, the court is free to treat this as somewhat of a blank canvas, bound only by First Amendment jurisprudence that has never been applied to laws such as these. Finally, this issue gets to the root of the conservative vitriol towards Section 230. Sure, conservative judges have criticized the broad immunity shield in §§ (c)(1), 403 however the conservative party as a whole seems more critical of §§ (c)(2).404 If the conservatives on the court were to take a more activist approach to Section 230 interpretation, they may be more likely to do it in these cases, as opposed to a case that focuses on §§ (c)(1).

E. Potential Solutions Moving Forward

In addition to Moody and Paxton, other Section 230 cases are sure to follow the Gonzalez decision. The debate on Silicon Valley censorship is only heating up as we move further into the age of the internet. As I'm writing this article, conservative politician Marjorie Taylor Greene has had her Twitter account suspended due to comments regarding Transsexuals and the Nashville Shooting on March 27th.405 She is the only the most recent in a long line of politicians to become upset with the platform over censorship.406 This is still occurring after First Amendment champion and activist billionaire Elon Musk purchased twitter last year in hopes of restoring “free speech” to the platform.407 Undoubtedly, these competing interests between free speech and content moderation will come to a head soon. Moreover, artificial intelligence is advancing at a rapid pace and litigation over whether it is immunized by Section 230 is certain to arise at some point.408 It is conceivable that, in under 20 years, AI will be recommending nearly everything to us, including what to eat for dinner, when to change lanes on the highway, and

---

402. See supra note 240.
403. See supra notes 148–49.
404. See supra Section I.D.
406. See supra note 147–62.
408. See supra note 284.
what to say when our boss asks why we were 20 minutes late this morning. At some point, we're likely to need a clear answer on whether tech firms are immunized for their AI recommendations.

What truly needs to happen is that Congress needs to step in and clarify what it now intends Section 230(c)(1) and (c)(2) to mean. We are currently applying a statute that was written at a time when the writers could not have conceived of the internet as it is today. The “twenty-six words that created the internet” may now need to be closer to twenty-six hundred words to encompass the breadth of modern technology. Even Chris Cox, one of the fathers of Section 230, has said that congress must “restat[e] the clear intent of Section 230, and reemphasiz[e] the plain meaning of its language that denies protection to internet platforms even partly complicit in the creation or development of illegal content.”

This is not a novel concept, as Congress has acted in this manner before. For example, with the passing of the Mann Act in 2018, they gave express exemptions from immunity for interactive computer services that conspire to promote prostitution. Similarly, Congress could create an express exemption to immunity for interactive computer services who do not use “neutral” algorithms and artificial intelligence or an exemption for platforms who do not take certain measures to remove specified user content—like child pornography or terrorist content.

Social media companies can take control of the situation by adopting their own measures too. “On balance...platforms—and not the government—are better suited to be the gatekeepers of online speech.” This is due to basic capitalist economic principles that platforms that are full of filth or who do not properly engage in content moderation will be overtaken by those that do. One way for platforms to take action would be to allow users to opt-in or out of algorithm and AI recommendations or to select from a host of options for content recommendation. This would take the publishing-like activities away from the platform itself and would place the liability for having “editorial control” over the recommendations with the user.

---

409. See supra note 284.
410. See generally 26 WORDS, supra note 1.
411. Id. at 268.
412. Id. at 270.
413. Id. at 249.
414. Id.
415. All-In with Chamath, Jason, Sacks & Friedberg, E116: Toxic Out-of-Control Trains, Regulators, and AI, at 48:50–52:00 (downloaded using Spotify).
who chose to use that specific algorithm. While this position has never been expressly adopted by a court, it would certainly attenuate the “creation and “development” aspects of content recommendations, and would arguably do enough to place responsibility with the user that chose the algorithm.

CONCLUSION

In sum, the importance of Section 230 to our modern society cannot be understated. Arguably no statutory law has had such a wide-ranging impact. Unfortunately, the interpretation of Section 230 has become a hotly debated topic, with some calling for a narrower interpretation and others advocating for the status quo. However, limiting the liability shield contained in Section 230 would be a mistake. Not only would it stifle innovation and free speech, but it could also lead to a wasteland where platforms are full of either curated “happy talk” or, conversely, pervasive filth. Instead, it is time for Congress to step in and clarify the scope of Section 230 immunity. This would provide certainty for tech companies, while also ensuring that they are held accountable for their actions. It is important that we recognize the crucial role that Section 230 has played in the development of the internet and that we work to ensure that it continues to foster innovation and free speech in the years to come.

416. Id.