IMMUNIZING THE ALGORITHM ONLY AS MUCH AS IT NEEDS: RETHINKING HOW COURTS ANALYZE ALGORITHMS UNDER SECTION 230

Andra Cernavskis†

TABLE OF CONTENTS

DOI: https://doi.org/10.15779/Z38028PG3C

† Andra Cernavskis is a 3L at University of California, Berkeley, School of Law. Before attending law school, she was a journalist and worked on news teams at various technology companies, including Twitter (now known as "X"). I'd like to extend my gratitude to my professors Allison Schmitt, Wayne Stacy, and Kenneth Bamberger, who helped me form ideas and challenged me in all the ways I needed it. I would also like to thank my colleagues Gaurav Lalsinghani, Michelle D'Souza, Alexis Tatum, Karina Sanchez, and William Clark, who provided me with invaluable feedback throughout the writing process. I would also like to thank my wonderful friends and family who understood how important this process was to me and supported me throughout.

I. INTRODUCTION

Anyone who has used social media—whether that's TikTok, Instagram, YouTube, or any other popular platform—has engaged with "the algorithm."[1]

1. In 2022, seven out of ten Americans used social media in some capacity. Lee Rainie, Cary Funk, Monica Anderson & Alec Tyson, *Mixed Views About Social Media Companies Using Algorithms to Find False Information*, PEW RSCH. CTR. (Mar. 17, 2022), https://

Social media users often talk about the algorithm's role in their lives and social media experiences, and many have tried to understand how it works or why particular content appears on their social media feeds. Whether people like it or not, the algorithm has a lot of power in modern society. It helps inform spending habits, what news users consume, what opinions people are exposed to, and even what hobbies or interests people adopt. This all happens through a type of algorithm known as a recommendation system. As Michael Schrage notes, "[m]uch as steam engines energized the Industrial Age, recommendation engines are the prime movers digitally driving 21st-century advice worldwide."[2] The algorithm is often characterized as an obscure, all-powerful deity that perhaps knows a person better than they know themselves.[3] That is to say, the algorithm has taken on a life of its own in the modern world.

However, "the algorithm" is not just one all-knowing, powerful entity, even if it sometimes feels like that might be the case. Companies that use algorithms—which extend far past social media companies and include online marketplaces like Amazon, streaming services like Netflix, and beyond[4]—all have their own individual algorithms that their own engineers built and maintain.[5] On top of that, all major companies use many different algorithms to perform different functions and reach different goals.[6] For example, one company may use one algorithm (or group of algorithms) for recommending content to a user while using another algorithm to filter out spam-type content from entering people's feeds.[7]

In its most simple form, algorithms are "a list of rules to follow in order to complete a task or solve a problem."[8] By this definition, recipes or directions

www.pewresearch.org/internet/2022/03/17/mixed-views-about-social-media-companies-using-algorithms-to-find-false-information/.

2. Michael Schrage, *The Recommender Revolution*, MIT TECH. REV. (Apr. 27, 2022), https://www.technologyreview.com/2022/04/27/1048517/the-recommender-revolution/.

3. *See generally* Eleanor Cummins, *The Creepy TikTok Algorithm Doesn't Know You*, WIRED (Jan. 3, 2022), https://www.wired.com/story/tiktok-algorithm-mental-health-psychology/.

4. *See* Rachel Metz, *Algorithms Are Everywhere. Here's Why You Should Care*, CNN (Nov. 19, 2021), https://www.cnn.com/2021/11/19/tech/algorithm-explainer/index.html; *see also* Larry Hardesty, *The History of Amazon's Recommendation Algorithm*, AMAZON SCI. (Nov. 22, 2019), https://www.amazon.science/the-history-of-amazons-recommendation-algorithm.

5. *See* Arvind Narayana, *Understanding Social Media Recommendation Algorithms*, KNIGHT FIRST AMEND. INST. AT COLUM. U. (Mar. 9, 2023), https://knightcolumbia.org/content/understanding-social-media-recommendation-algorithms.

6. *See generally* Rainie et al., *supra* note 1.

7. *See generally id.*

8. *What Is an Algorithm?,* BBC, https://www.bbc.co.uk/bitesize/articles/z3whpv4 (last visited May 5, 2025).

to a friend's house are all algorithms.[9] These are classic, rule-based algorithms, and these types of algorithms can and do exist on digital platforms.[10] However, rule-based algorithms are difficult to scale because they are largely hand-coded. While hand-coding algorithms makes the algorithm easier to understand and therefore troubleshoot when needed, it also means that if individual developers' were to create rule-based algorithms to fuel social media feeds, the engineers' assumptions about what people want to see online would be baked into the rules of those algorithms, whether those assumptions are correct or not.[11]

Therefore, most of the algorithms that now fuel the modern online experience are machine-learning recommendation algorithms, which are also known as recommender systems.[12] These algorithms all share at least one feature in that they are built using advanced machine-learning models that are trained on massive data sets that effectively teach the system how to make predictions based on that data or classify data in an organized way.[13] In this way, recommender systems are a lot more complex than rule-based algorithms. In fact, experts often accuse these types of algorithms as being black boxes because of the nearly impossible task of understanding how and why they work the way they do.[14]

For many users, recommendation systems make their social media experience more pleasurable, offering up entertaining or educational content related to their specific interests. However, it is no secret that there is a dark side to social media companies' use of recommendation systems. The world discovered this after the 2016 U.S. presidential election, when whistleblowers and researchers shined a light on how these types of algorithms manipulated voter behavior and spread election misinformation.[15] Since then, social media companies that use recommendation algorithms have been accused of

9. *See id.*

10. *See* Chris Meserole, *How Do Recommender Systems Work on Digital Platforms?*, BROOKINGS (Sep. 21, 2022), https://www.brookings.edu/articles/how-do-recommender-systems-work-on-digital-platforms-social-media-recommendation-algorithms/.

11. *See id.*

12. *See id.*

13. *See* Simson L. Garfinkel, *A Peek at Proprietary Algorithms*, AM. SCIENTIST, https://www.americanscientist.org/article/a-peek-at-proprietary-algorithms.

14. *See* Cynthia Rudin & Joanna Radin, *Why Are We Using Black Box AI When We Don't Need To? A Lesson from an Explainable AI Competition*, HARV. DATA SCI. REV. (Nov. 22, 2019), https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/8.

15. *See generally* Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

radicalizing terrorists, promoting eating disorders to at-risk, young girls, spreading more dangerous misinformation, and promoting hate speech.[16]

Despite the extreme power and influence that recommendation algorithms hold in modern society, the companies responsible for building and maintaining these algorithms have been able to do so with very little oversight or government regulation. This is all because of one federal law that is often credited with creating the internet as we know it today in the United States: § 230.[17] Congress passed § 230 in 1996 when it saw a growing need to encourage the creation and development of internet companies.[18] While § 230 has many components, there are twenty-six words that carry the most weight and have received the most attention: "[n]o 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."[19] These are the words that have allowed multitudes of internet companies to invoke statutory immunity as a defense when a plaintiff seeks damages for harms related to content posted by third parties on websites, including content that was promoted by the company's own recommendation algorithms.[20]

While it was relatively uncontroversial at the time of its enactment, § 230 has remained statutorily unchanged since 1996. This is despite both the facts that the internet looks completely different than it did in 1996 and that § 230 arguably finished its intended job in promoting innovation and U.S. internet company growth. The companies that the law originally sought to help are now some of the wealthiest and most powerful corporations in the world.[21] Despite

16. *See* John Schultz, *The Drivers of Platform Harm*, BELFER CTR. FOR SCI. & INT'L AFFS. (June 5, 2023), https://www.belfercenter.org/publication/drivers-platform-harm; *Deadly By Design: TikTok Pushes Harmful Content Promoting Eating Disorders and Self-Harm Into Users' Feeds*, CTR. FOR COUNTERING DIGIT. HATE (Dec. 2022), https://counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf; *Five Things About the Role of the Internet and Social Media in Domestic Radicalization*, NAT'L INST. JUST. (Dec. 18, 2023), https://nij.ojp.gov/topics/articles/five-things-about-role-internet-and-social-media-domestic-radicalization; *see generally* Pilar M. Hoye, *Down the Alt-Right Rabbit Hole: The Role of Social Media Platforms in the Radicalization of Domestic Right-Wing Terrorists,* 33 S. CAL. INTERDISC. L.J. 161 (2023).

17. *See* Stephen Engelberg, *Twenty-Six Words Created the Internet. What Will It Take to Save it?*, PROPUBLICA (Feb. 9, 2021), https://www.propublica.org/article/nsu-section-230.

18. *See* VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., R46751, SECTION 230: AN OVERVIEW 2 (2024).

19. 47 U.S.C. § 230(c)(1).

20. Alan Z. Rozenshtein, *Interpreting the Ambiguities of Section 230*, BROOKINGS (Oct. 26, 2023), https://www.brookings.edu/articles/interpreting-the-ambiguities-of-section-230/#liability-for-algorithmic-amplification-754.

21. *See* Letter from William P. Barr, Att'y Gen., United States, to Michael R. Pence, President, United States Senate (Sep. 23, 2020), https://www.justice.gov/ag/media/1093246/

modern realities, both legislative and judicial branches in the United States have had a difficult time adapting the 1996 law to a rapidly changing internet. As such, § 230 has remained a consistent shield for large internet companies to protect them from liability for harmful content on their platforms, which now includes content that may connect individuals with terrorist organizations or help convince a young girl to develop an eating disorder. As the internet has grown and developed in the decades since Congress passed § 230, the question of what § 230 continues to protect has taken center stage with one of the most important questions currently being: Does § 230 apply to recommendation algorithms?[22] Furthermore, the question of how far § 230 will go is becoming ever more critical in the face of the rapid technological advancements being made with generative AI.

On top of § 230 remaining unchanged in the light of modern realities, U.S. courts have also overgeneralized the function of social media platforms and algorithms under § 230. Throughout many of the cases that address how § 230 applies to social media companies' algorithms, federal courts have treated these algorithms as one, monolithic entity that works roughly the same way across and within companies. This results in an all-or-nothing approach in which algorithms, as a single concept, are determined to either violate § 230 or not. This all-or-nothing approach leaves little room for courts to consider that some algorithms may violate § 230, while others do not. Instead, courts should consider taking a much narrower, more fact-intensive approach to determining § 230 immunity and liability. This new approach should examine each individual algorithm separately from other algorithms on the same or different platforms. If this individualized approach is taken, courts can assess a single algorithm under the law and find it to be outside the scope of § 230 immunity without over-implicating other algorithms within the same platform or across platforms.

Part II of this Note will first examine the legislative and judicial background of § 230 and why recommendation algorithms have posed a unique challenge for courts when examining § 230 as a defense. Part III will

---

dl?inline= [https://perma.cc/R42E-A2TE]; *see also* Engelberg, *supra* note 17 (referring to the title of Jeff Kosseff's book, *The Twenty-Six Words That Created the Internet*); Andrea Murphy & Matt Schifrin, *The Global 2000 2024*, FORBES (June 6, 2024), https://www.forbes.com/lists/global2000/; Alina Sekyukh, *Section 230: A Key Legal Shield for Facebook, Google Is About to Change*, NPR (Mar. 21, 2018), https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change.

22. Other important debates involve § 230's role in protecting free speech and promoting thoughtful content moderation practices. Jennifer Stisa Granick, *Is This the End of the Internet as We Know It*, ACLU (Feb. 22, 2023), https://www.aclu.org/news/free-speech/section-230-is-this-the-end-of-the-internet-as-we-know-it.

then expand on some of the key appellate and Supreme Court cases that have characterized algorithms either in a § 230 analysis or otherwise.[23] Part IV will address faults with the courts' broad characterizations of algorithms, propose a new, more fact-intensive and individualized approach for courts to take that will result in more satisfying outcomes for plaintiffs and defendants alike, and address potential concerns with the new approach (such as the potential for chilling speech and how the new approach might be implemented). Finally, Part V will conclude and suggest how the new approach introduced in Part IV could be helpful in future cases that surely will involve new and developing technologies beyond the recommendation algorithm.

II. THE DEVELOPMENT OF SECTION 230

Part II will first address the legislative and early judicial history of § 230, paying special attention to key cases that have helped shape appellate courts' broad understandings of the statutory language. Part II will then examine more recent appellate court cases that have either limited the initial broad interpretation of § 230 over the years or helped define a test for how to apply § 230 to various claims against internet companies. Lastly, Part II will address why § 230 poses a unique challenge when it comes to emerging technologies that did not exist when Congress passed the statute, namely recommendation algorithms.

A. SECTION 230

Section II.A will first examine the legislative history and goals of § 230 in the context of the 1996s internet. Section II.A will also address the debates that have arisen because § 230 has remained unchanged for nearly 30 years. The discussion will then turn to the early judicial interpretation of § 230 in *Zeran v. America Online, Inc.*, decided shortly after Congress passed § 230.[24] In *Zeran,* the Fourth Circuit broadly interpreted how much immunity internet companies should receive under the statute when it was presented with a case in which a plaintiff was seeking to hold AOL accountable for harmful content posted by a third-party user.[25] *Zeran*'s broad interpretation of § 230 has since influenced courts' § 230 analysis for decades, for better or worse.[26]

23. If the Supreme Court decides to take up the § 230 issue of how the law is applied to algorithms, the Court's already-existing characterization of algorithms could influence its future decisions.

24. *See generally* Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).

25. *See generally id.*

26. *See* Rozenshtein, *supra* note 20.

1. *Legislative History*

The internet has changed dramatically since it started to become widely available to the public in the 1990s. Section 230 passed at a time when the internet was beginning to take off. For example, in the year prior to § 230's enactment, only 21 percent of people in the U.S. had used the internet.[27] A year later, that number grew to 73 percent.[28] Congress passed § 230, in part, to promote the growth of the technology industry and shield internet companies from lawsuits that could potentially put them out of business.[29] Known as "the twenty-six words that created the internet,"[30] § 230 of the Communications Decency Act (CDA) has been highly impactful ever since Congress passed it in 1996.

Congress initially passed § 230 as part of a group of measures meant to amend the Communications Act of 1934.[31] The group of new measures was collectively known as the CDA and was largely enacted to protect children on the internet from pornography and obscene materials.[32] Section 230, however, stood apart from many of the other sections of the CDA. While the Supreme Court quickly struck down most of the CDA on First Amendment grounds, § 230 remains the only constitutionally sound part of the CDA.[33]

Congress passed § 230 largely in response to a 1995 New York state court decision in *Stratton Oakmont, Inc. v. Prodigy Services Co.*, which held that an internet company was liable for libelous statements a user had posted to its message boards.[34] Congress wanted to provide immunity to internet companies like Prodigy Services from liability for third-party content posted on their platforms.[35] The idea was that if companies were embattled in endless litigation over the legality of third-party content, they would not be able to grow and innovate in any meaningful way.[36] The provision granting internet companies immunity for third-party content can mostly be found in subsection (c)(1) of § 230, which states, "[n]o provider or user of an interactive computer

27. *News Attracts Most Internet Users: Online Use*, PEW RSCH. CTR. (Dec. 16, 1996), https://www.pewresearch.org/politics/1996/12/16/online-use/.

28. *Id.*

29. JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 57–78 (2019).

30. Engelberg, *supra* note 21 (referring to the title of Jeff Kosseff's book, *The Twenty-Six Words That Created the Internet*).

31. *See* BRANNON, *supra* note 18, at 1.

32. *Id.*

33. *See id.*

34. *See* Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 *5 (N.Y. Sup. Ct. May 24, 1995).

35. *See* BRANNON, *supra* note 18, at 7.

36. *See* Barr, *supra* note 21.

service shall be treated as the publisher or speaker of any information provided by another information content provider."[37] Subsection (c)(1) is also the focus of the debates surrounding § 230.[38]

Another important goal of § 230 was to allow internet companies to moderate the content on their websites without fear of liability if they act "in good faith."[39] As Jeff Kosseff, a well-known proponent of § 230, says, "[t]oday it protects both from liability for user posts as well as liability for any claims for moderating content."[40]

There is an ongoing debate about whether § 230 remains a necessary law, given modern realities. Although often with different motives, elected officials and politicians from across the aisle have argued that § 230 has run its course and that social media companies are abusing the law in order to protect themselves in situations where they should be held liable.[41] As such, many have recently called for § 230 reform or for its repeal entirely.[42] So far, none of these efforts have been effective.[43] Proponents of § 230 continue to argue that without the law in its current form, the internet we know today could not exist.[44] Regardless of where one stands on § 230, one thing is clear: it has remained on the books since 1996 fairly unscathed.

2. *Early Judicial Interpretation in* Zeran v. America Online, Inc. *(1997)*

In the years and decades since 1996, many have attempted to use the courts to hold internet companies responsible, at least in part, for disseminating and potentially contributing to harmful content on their platforms. However, these efforts have had little success because judges often find that § 230 bars

37. 47 U.S.C. § 230(c)(1).

38. Danielle Draper, *Summarizing the Section 230 Debate: Pro-Content Moderation vs. Anti-Censorship*, BIPARTISAN POL'Y CTR. (July 5, 2022), https://bipartisanpolicy.org/blog/summarizing-the-section-230-debate-pro-content-moderation-vs-anti-censorship/.

39. 47 U.S.C. § 230(c)(2)(a); Barbara Ortutay, *What You Should Know About Section 230, The Rule That Shaped Today's Internet*, PBS (Feb. 21, 2023), https://www.pbs.org/newshour/politics/what-you-should-know-about-section-230-the-rule-that-shaped-todays-internet.

40. Ortutay, *supra* note 39.

41. *E.g.*, Sara Morrison, *Section 230, The Internet Law That's Under Threat, Explained*, VOX (Feb. 23, 2023), https://www.vox.com/recode/2020/5/28/21273241/section-230-explained-supreme-court-social-media.

42. ERIC N. HOLMES, CONG. RSCH. SERV., R47753, LIABILITY FOR ALGORITHMIC RECOMMENDATIONS 14 (2023).

43. *Id.*

44. *Section 230*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/cda230 (last visited Dec. 18, 2024); Granick, *supra* note 22.

plaintiffs' claims.[45] This is due largely to the early judicial interpretation of § 230, which construed immunity under the statute to be very broad.[46]

Zeran v. America Online, Inc. was the first case to interpret § 230 in 1997, shortly after the CDA passed.[47] The Fourth Circuit decided in favor of AOL, ruling that § 230(c) "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[48] The case involved an unknown America Online user who had tried to sell t-shirts containing offensive slogans referring to the Oklahoma City bombing. The unidentified user's post provided the phone number of plaintiff Zeran as a way for people to order the shirts. Zeran received threatening telephone calls because of this user's post, and he consequently sued AOL for defamation.[49]

The Fourth Circuit, interpreting the legislative intent of § 230 and the plain language of the statute, said that § 230(c)(1) makes it so that any "computer service provider" is "plainly immunize[d]" from being held liable for "information that originates with third parties."[50] While later opinions noted that subsection (c)(1) does not mention the term "immunity," the Fourth Circuit interpreted (c)(1) to provide broad immunity for internet companies when it comes to hosting third-party content on their websites.[51] That is, most internet companies would not be held liable for any third-party content posted on their websites, according to *Zeran*.[52] Importantly, § 230(c)(1) does not protect internet companies from claims based on the company's own, original content.[53]

The *Zeran* opinion also weighed in on the term "publisher" included in § 230(c)(1). It said § 230 "precludes courts from entertaining claims that would place a computer service provider in a publisher's role."[54] The Fourth Circuit further defined what it means to serve a publishing role, saying that it includes "traditional editorial functions . . . such as deciding whether to publish, withdraw, postpone or alter content."[55] Here, the Fourth Circuit opined that

---

45. *See generally Zeran*, 129 F.3d.
46. *See generally id.*
47. *Id.*
48. *Id.* at 330.
49. *Id.* at 328–29.
50. *Id.* at 330.
51. Barnes v. Yahoo! Inc., 570 F.3d 1096, 1100 (9th Cir. 2009); Chi. Laws.' Comm. for C.R. Under L., Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008).
52. *See Zeran*, 129 F.3d at 335.
53. BRANNON, *supra* note 18, at 16.
54. *Zeran*, 129 F.3d at 330.
55. *Id.*

without this type of publisher immunity, internet companies would be disincentivized to self-regulate.[56] It noted that Congress passed § 230 in part to allow companies to self-regulate third-party content—what is referred to today as "content moderation"—without fear of liability for those decisions.[57] Since *Zeran*, other courts of appeal have largely adopted the Fourth Circuit's broad interpretation of § 230(c)(1) and its explanation of the term "publisher."[58]

B. IMPORTANT SECTION 230 CASES POST-*ZERAN*

Section II.B will discuss two landmark Ninth Circuit cases that qualified the broad § 230 immunity established in *Zeran*: *Fair Housing Council v. Roommates.com* and *Barnes v. Yahoo!*.[59] These two cases established the two most important tests courts now use in analyzing § 230 immunity against claims. *Roommates.com* established the material contribution test, which says that for a company to be held liable for unlawful content posted to their platforms, that company must have helped co-develop that content in a way that contributes to its illegality.[60] *Barnes* established a namesake three-part test that plaintiffs' claims must meet to survive a motion to dismiss against a § 230 immunity defense.[61] Courts now almost exclusively rely on these tests when determining § 230 immunity. Section II.B will lastly explain how these tests work together.

1. Fair Housing Council v. Roommates.com *(2008)*

Fair Housing Council v. Roommates.com was the one of the first cases to qualify the broad § 230 immunity established in *Zeran* over twenty years after *Zeran*. The Ninth Circuit held that Roommates.com was liable under § 230 for third-party content posted to its website that it had in part developed.[62] Plaintiffs successfully alleged that the website had violated aspects of the Fair Housing

56. *See id.* at 331.

57. BRANNON, *supra* note 18, at 16.

58. *See, e.g.*, Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019); *Barnes*, 570 F.3d at 1096. *But see* BRANNON, *supra* note 18, at 11 (noting that "some jurists have expressed skepticism about the Fourth Circuit's approach. In a statement written to accompany a denial of certiorari in a § 230 case, U.S. Supreme Court Justice Clarence Thomas suggested, contrary to the holding in *Zeran*, that § 230(c)(1) might not limit distributor liability. Two federal appellate judges concurring in separate § 230 cases also questioned whether *Zeran*'s definition of 'publisher' interpreted § 230(c)(1) beyond its intended scope. In addition to the skepticism expressed by individual jurists, a 2022 Fourth Circuit opinion appeared to narrow *Zeran*'s conception of 'publisher' activity without disturbing its basic ruling on distributor liability.")

59. *See generally* Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157 (9th Cir. 2008); *Barnes*, 570 F.3d.

60. *See Roommates.com*, 521 F.3d at 1168.

61. *See Barnes*, 570 F.3d at 1100–01.

62. *See Roommates.com*, 521 F.3d at 1175.

Act when it asked its users to fill out a questionnaire in which they answered questions based on legally protected characteristics and subsequently displayed those answers on users' profiles.[63] The Ninth Circuit decided that the answers displayed on the users' profiles were not entirely third-party content because Roommates.com had helped develop, at least in part, the content and contributed to what made that content illegal.[64] This meant that Roommates.com could be held liable for illegal content in which it helped in part create: in this case the answers to the discriminatory questions published on users' profiles.[65]

The Ninth Circuit's decision created an important test. Chief Judge Kozinski articulated the appropriate test, holding: "a website helps to develop unlawful content . . . if it contributes materially to the alleged illegality of the conduct."[66] Following *Roommates.com*, the Ninth Circuit continued to clarify what has come to be known as the material contribution test in other opinions, including stating that the test "draw[s] the line at the 'crucial distinction between, on the one hand, taking actions (traditional to publishers) that are necessary to the display of unwelcome and actionable content and, on the other hand, responsibility for what makes the displayed content illegal or actionable.'"[67]

The Ninth Circuit looked to the statutory text of § 230(f)(3) in forming the material contribution test.[68] Section 230(f)(3) defines "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[69] Section 230(f)(3)'s definition of "information content provider" has led to courts, when analyzing third-party content, largely "focus[ing] on the defendant's role in the 'creation or development' of the content."[70] The Ninth Circuit noted in *Roommates.com* that only holding companies liable when they are co-developers of third-party content ignores the "in part" phrasing of the passage in the statute that reads "creation or development in whole or in part."[71] The Ninth Circuit stated that

63. *See id.* at 1161.
64. *See id.* at 1172.
65. *See id.* at 1175.
66. *Id.* at 1168.
67. Kimzey v. Yelp! Inc., 836 F.3d 1263, 1269 n.4 (9th Cir. 2016) (quoting Jones v. Dirty World Ent. Recordings LLC, 755 F.3d 398, 413–14 (6th Cir. 2014)).
68. *Roommates.com*, 521 F.3d at 1166.
69. 47 U.S.C. § 230(f)(3).
70. BRANNON, *supra* note 18, at 16.
71. Max Del Real, Note, *Breaking Algorithmic Immunity: Why Section 230 Immunity May Not Extend to Recommendation Algorithms*, 99 WASH. L. REV. ONLINE 1, 18 (2024); *Roommates.com*, 521 F.3d at 1167 (quoting 47 U.S.C. § 230(f)(3)).

when platforms act as "passive conduits," they should receive § 230 immunity for any third-party content posted to their sites.[72] However, full immunity does not always extend to co-developers, especially when they "materially contribute" and therefore "in part" develop the offending content.[73] The Ninth Circuit also said that when platforms provide "neutral tools" to users, it does not mean that the platform itself is acting as a developer of content, and the platform should therefore still receive § 230 immunity for third-party content it might display through these neutral tools.[74] The court defined "neutral tools" to be those that are "identically applied in all contexts."[75]

The court's decision in *Roommates.com* was truly ground-breaking in how it interpreted § 230 and its willingness to draw a line when it comes to extending the statute's immunity for different types of content. Under the material contribution test, platforms can be held liable more often than they had been prior to the *Roommates.com* opinion.[76]

2. Barnes v. Yahoo! *(2009)*

Shortly after *Roommates.com* established the material contribution test, another Ninth Circuit opinion established a now widely used three-part legal test to determine if a defendant is liable under § 230. In *Barnes v. Yahoo!*, the Ninth Circuit held that § 230 barred the plaintiff's claims because Yahoo! performed traditional publishing functions when it hosted and failed to take down third-party content posted by the plaintiff's ex-boyfriend as a means of revenge.[77] The plaintiff, Barnes, wanted to hold the internet company that hosted the content, Yahoo!, liable under Oregon tort law for what the Ninth Circuit synthesized as "negligent undertaking."[78]

The Ninth Circuit found that § 230 does not "declare[] a general immunity from liability deriving from third-party content," which was what Yahoo! argued.[79] With this sentiment established, the Ninth Circuit interpreted both § 230(c)(1) and § 230(e)(3) to develop what is now widely known as the *Barnes* test.[80] The test states that "(c)(1) *only* protects from liability (1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat,

72. *Roommates.com*, 521 F.3d at 1167.
73. *Id.*
74. *See id.* at 1169.
75. Del Real, *supra* note 71, at 20.
76. *See* G.S. Hans, *Revisiting Roommates.com*, 36 BERKELEY TECH. L.J. 1227, 1230 (2021).
77. *See Barnes*, 570 F.3d at 1103.
78. *Id.* at 1099 (discussing the unclear nature of plaintiffs' negligence claim under Oregon tort law).
79. *Id.* at 1100.
80. *Id.* at 1100–01.

under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider."[81]

Courts now almost ubiquitously rely on *Barnes*, or the three-part immunity test, and material contribution tests to dismiss claims on § 230 grounds. For a claim to pass the three prongs of the *Barnes* test and therefore receive § 230 immunity, plaintiffs need to prove that one of the three prongs is not satisfied: (1) the defendant is an interactive computer provider or user (2) whom the plaintiff seeks to treat as a publisher or speaker (3) of information provided by a third-party information content provider.[82] Once the court finds that the test has been met, no additional factfinding occurs.[83] In terms of the material contribution test and neutral tools framework established in *Roommates.com*, they are best understood as working in tandem with Prong Three of the *Barnes* test.[84] An internet company's § 230 defense is likely to fail Prong Three of the *Barnes* test if two conditions are met. The first condition is met when an internet company is found to materially contribute to the third-party, offending content in question. The second condition is met when a platform is found to have encouraged the third party's posting of illegal content rather than hosting all content neutrally.[85] If the content in question meets both of these conditions, it is unlikely to pass Prong Three of the *Barnes* test, and the company therefore is likely to be held liable for the offending content under § 230.[86]

C. RECOMMENDATION ALGORITHMS AND SECTION 230

As internet companies have grown and developed since 1996, in no small part due to the freedom from litigation that § 230 has afforded them, they have developed increasingly sophisticated tools that interact with third-party content. These new tools have posed novel and challenging questions about how far § 230 immunity extends. One of these tools is recommendation systems. Recommendation systems are now a common type of algorithm used by companies to predict and sort content that is presented to users. They are the algorithms that this Note will mostly address.

Recommendation systems are based on machine-learning models that "use[] data to help predict, narrow down, and find what people are looking for

81. *Id.* (emphasis added).
82. Lemmon v. Snap, Inc., 995 F.3d 1085, 1091 (9th Cir. 2021).
83. Del Real, *supra* note 71, at 9.
84. *See* Gonzalez v. Google LLC, 2 F.4th 871, 892–93 (9th Cir. 2021).
85. *Id.*
86. *Id.*

among an exponentially growing number of options."[87] The data that recommendation systems (also known as recommendation algorithms) use to train themselves to better understand individual users can include demographic information, search history, a user's engagement with other content on a platform, and other various factors.[88] By using these various inputs from individual users, an algorithm teaches itself what a user might like and attempts to provide users with, as the name suggests, recommendations for more of what they like or what the machine thinks they might like.[89] While most recommendation algorithms are built on the above-discussed premise, there are many different types of recommendation algorithms that use different inputs and prioritize different filtering systems to provide individuals with personalized recommendations.[90] For example, Instagram's "Feed" has traditionally prioritized content posted by users that someone has actively chosen to follow, whereas TikTok's For You Page famously does not prioritize content from users someone has chosen to follow.[91] Additionally, each of these recommendation systems—Instagram's "Feed," TikTok's For You Page, and all the comparable tools on other platforms—is made up of many different algorithms that accomplish different goals.[92] Computer scientists refer to the collection of individual algorithms that fuel each of the systems mentioned above as "recommender systems."[93]

As more internet companies build algorithms or systems of algorithms and as those algorithms or systems become more complex, courts have had to increasingly contend with whether companies should be held legally liable for recommending content through recommendation systems.[94] For the purposes of this paper, "recommendation systems" and "recommendation algorithms" will mean the same thing in that they will both refer to the system of algorithms that makes up an overall recommending experience. As such, the algorithms that make up each recommendation system can be considered individual parts of the larger system.

87. *Recommendation System*, NVIDIA, https://www.nvidia.com/en-us/glossary/recommendation-system/ (last visited Dec. 18, 2024).

88. *Id.*

89. *Id.*; Schrage, *supra* note 2.

90. *Recommendation System*, *supra* note 87.

91. HOLMES, *supra* note 42, at 3.

92. *See, e.g.*, Karen Hao, *The Facebook Whistleblower Says Its Algorithms Are Dangerous. Here's Why.*, MIT TECH. REV. (Oct. 5, 2021), https://www.technologyreview.com/2021/10/05/1036519/facebook-whistleblower-frances-haugen-algorithms/.

93. HOLMES, *supra* note 42, at 3.

94. *Id.* at Summary.

III. RECOMMENDATION ALGORITHMS IN THE COURTS

Part III will examine how two appellate courts came to the same decision about recommendation algorithms' role in assisting in terrorism. Both courts applied the *Barnes* and material contribution tests to recommendation algorithms and barred plaintiffs' claims under § 230, setting the stage for other courts' analysis of recommendation algorithms and § 230 immunity. Part III will then examine how the Supreme Court has characterized algorithms in two opinions outside of the § 230 context, which has already influenced how lower courts characterize algorithms within the § 230 context. Lastly, Part III will examine how one appellate court recently came to a different conclusion from the other appellate courts when examining recommendation algorithms under § 230, signaling a circuit split.

A. *FORCE V. FACEBOOK* (2019)

The Second Circuit's opinion in *Force v. Facebook* is one of the most important cases covering recommendation algorithms under § 230.[95] It is important because the decision was the first federal appellate decision to hold that § 230 bars civil terrorism claims against social media companies' use of recommendation algorithms.[96] The case centered on a series of terrorist attacks executed by Hamas against five Americans in Israel from 2014 to 2016.[97] Plaintiffs alleged that Facebook violated federal anti-terrorism laws both by allowing Hamas to post content that encouraged the attacks and also by recommending that Hamas-created content to the people who carried out the attacks through its recommendation algorithm.[98] Plaintiffs further alleged that Facebook contributed to Hamas's content through its recommendation algorithm.[99] Facebook, in turn, argued that § 230 barred all the claims against it, including ones involving its algorithm§ 230.[100] The Second Circuit agreed with Facebook and held that § 230 barred plaintiffs' claims that Facebook went beyond its role as publisher through the use of its algorithms and materially contributed to the offending content through its algorithm.[101]

95. *See generally Force*, 934 F.3d.

96. Sophia Cope & Aaron Mackey, *Second Circuit Rules That Section 230 Bars Civil Terrorism Claims Against Facebook,* ELEC. FRONTIER FOUND. (Aug. 7, 2019), https://www.eff.org/deeplinks/2019/08/second-circuit-rules-section-230-bars-civil-terrorism-claims-against-facebook.

97. *Force*, 934 F.3d at 57.

98. *Id.* at 59.

99. *Id.* at 62.

100. *See id.* at 57.

101. *See id.* at 70–71.

The Second Circuit examined Hamas's content on Facebook through the *Barnes* test.[102] The second prong of the *Barnes* test asks: does a plaintiff seek to treat the defendant as a publisher or speaker?[103] Under this second prong, the Second Circuit decided that plaintiffs' claims treated Facebook as a publisher, even when plaintiffs were arguing the opposite, because they were seeking to hold Facebook liable for performing traditional publishing activities.[104] Even though plaintiffs argued that Facebook did not act as a publisher when it came to its use of recommendation algorithms, the Second Circuit found that Facebook acted as a publisher when employing a recommendation algorithm because of the algorithm's traditional publishing functions of "arranging and distributing third-party information."[105]

Additionally, under the third prong of the *Barnes* test and, consequently, the material contribution test, the Second Circuit held that Facebook did not materially contribute to the content Hamas posted, even when it recommended that content to potential Hamas recruits through its algorithm.[106] The Second Circuit said that Facebook merely displayed the objectionable content rather than played a role in what made that displayed content illegal or objectionable.[107] The Second Circuit stated that if Facebook were to have done something like instruct Hamas on how to target its content to relevant audiences who were likely to carry out attacks, the platform might fail the material contribution test.[108] Thus, the Second Circuit found that plaintiffs' claims did not pass the *Barnes* and material contribution tests, and Facebook was shielded from liability under § 230.

While the Second Circuit extended § 230 immunity to Facebook's recommendation algorithm, Chief Judge Katzmann concurred in part and dissented in part, as he ultimately disagreed about whether § 230 immunity should extend to all of Facebook's algorithms.[109] While Chief Judge Katzmann agreed with the outcome of the majority's opinion, he specifically dissented on the majority's treatment of Facebook's "suggestion algorithms."[110] The Chief Judge presented a scenario that challenged the majority's opinion that

102. *Id.* at 65.
103. *Barnes*, 570 F.3d at 1100–01.
104. *Force*, 934 F.3d at 65.
105. *Id.* at 66.
106. *Id.* at 69 (2d Cir. 2019) (holding the difference between displaying illegal content and playing a role in what makes the displayed content illegal or actionable).
107. *See id.* at 70.
108. Different appellate courts took similar stances in other cases. *See generally* Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093 (9th Cir. 2019).
109. *Force*, 934 F.3d at 76. (Katzmann, C.J., concurring in part and dissenting in part).
110. *Id.*

Facebook acts as a publisher and that its algorithm is simply an extension of its role as a publisher in sorting and displaying the content posted to the website. He wrote:

> Suppose that you are a published author. One day, an acquaintance calls. 'I've been reading over everything you've ever published,' he informs you. 'I've also been looking at everything you've ever said on the Internet. I've done the same for this other author. You two have very similar interests; I think you'd get along.' The acquaintance then gives you the other author's contact information and photo, along with a link to all her published works. He calls back three more times over the next week with more names of writers you should get to know.[111]

Chief Judge Katzmann said that he would not find the acquaintance to be a "publisher" in this scenario.[112] Given that the acquaintance's activities mimic those of a recommendation algorithm, Chief Judge Katzmann argued that social media companies should not be treated as publishers when it comes to their recommendation algorithms performing similarly to the acquittance in the hypothetical.[113]

In fact, Chief Judge Katzmann wrote extensively that he would not extend § 230 immunity to Facebook's recommendation algorithm, which he called the "friend- and content-suggestion algorithm."[114] He suggested that while some aspects of social media platforms are like some aspects of traditional publishers, not all actions the platforms take should be considered to be similar to those a publisher takes.[115] He argued that § 230 "limits liability based on the function the defendant performs, not its identity."[116] Section 230, he argued, only immunizes social media companies from those activities that resemble traditional publisher functions but not the whole range of activities it engages in.[117] He also invoked the material contribution test and neutral tools framework as established in *Roommates.com* and directly quoted from that decision to suggest Facebook "'does not merely provide a framework that could be utilized for proper or improper purposes; rather, [Facebook's] work in developing' the algorithm and suggesting connections to users based on their prior activity on Facebook, including their shared interest in terrorism, 'is

111. *Id.*
112. *Id.*
113. *Id.* at 77. (Katzmann, C.J., concurring in part and dissenting in part).
114. *Id.*
115. *Id.* at 81–82 (Katzmann, C.J., concurring in part and dissenting in part).
116. *Id.* at 81 (Katzmann, C.J., concurring in part and dissenting in part).
117. *Id.*

directly related to the alleged illegality of the site.'"[118] Chief Judge Katzmann thus presented an alternative way to view algorithms in relation to § 230 in his dissent.

B. *GONZALEZ V. GOOGLE* (2021)

Gonzalez v. Google is another case that dealt with a plaintiff seeking to hold a social media company liable for aiding and abetting acts of terrorism through its recommendation algorithm.[119] Like the Second Circuit in *Force*, the Ninth Circuit held that § 230 barred plaintiffs' claims because Google acted as a publisher and did not materially contribute to the offending content.[120] The Supreme Court granted certiorari in *Gonzalez* but side-stepped the § 230 issues present in the case by issuing an opinion in a companion case, *Twitter v. Taamneh*, which resolved the terrorism-related torts claims without addressing § 230 immunity.[121] The discussion here will focus on the Ninth Circuit's decision, which did address the § 230 issues present in the case.

Gonzalez, like *Force*, dealt with claims that attempted to hold social media platforms responsible for their alleged roles in terrorist attacks under the Anti-Terrorism Act, and plaintiffs in both cases made the argument that platforms' recommendation algorithms "helped advance the cause of terrorist groups using the platforms."[122] In *Gonzalez*, plaintiffs sued Google, Twitter, and Facebook for alleged violations of the Anti-Terrorism Act, claiming the platforms had "allowed ISIS to post videos and other content to communicate the terrorist group's message, to radicalize new recruits, and to generally further its mission."[123] The plaintiffs were family members of people who were executed in an ISIS terrorist attack in Paris.[124]

Much like the Second Circuit in *Force*, the Ninth Circuit used the *Barnes* test in *Gonzalez* to find that § 230 immunity extended to YouTube's recommendation algorithm, owned by Google.[125] In its relatively quick Prong Two analysis, the Ninth Circuit relied on *Force* to hold that Google is a publisher under the *Barnes* test.[126] The Ninth Circuit then spent considerably more time on Prong Three and the material contribution test, ultimately holding that recommendation algorithms are afforded § 230 immunity

118. *Id.* at 83 (Katzmann, C.J., concurring in part and dissenting in part).
119. *See generally Gonzalez*, 2 F.4th.
120. *See generally Force*, 934 F.3d; *see also Gonzalez*, 2 F.4th at 892–97.
121. Twitter, Inc. v. Taamneh, 137 HARV. L. REV. 402 (2023).
122. BRANNON, *supra* note 18, at 9.
123. *Gonzalez*, 2 F.4th at 880.
124. *Id.* at 880–82.
125. *See id.* at 891–93.
126. *See id.* at 891.

because, by recommending third-party content to users, they are not materially contributing to the content in question.[127] The Ninth Circuit likened the Google video-sharing platform's (YouTube) recommendation algorithm to a traditional search engine.[128] While the court admitted that recommendation algorithms are "more sophisticated than traditional search engine[s] . . . the core principle is the same."[129] The court used this logic to suggest that Google "provide[s] a neutral platform that did not specify or prompt the type of content to be submitted, nor determine particular types of content its algorithms would promote."[130]

However, the concurrence in *Gonzalez* is worth noting for its similarities to the dissent in *Force*. In both the concurrence and dissent, Judge Berzon and Judge Gould explicitly invoked Chief Judge Katzmann's analysis in the *Force* dissent. Judge Berzon made it clear that the only reason she concurred with the judgement is because she found that the Ninth Circuit is "bound by [] precedent compelling the outcome in this case."[131] She urged the court to reconsider its precedent so that the "term" publisher under § 230 does not extend to machine-learning algorithms and "activities that promote or recommend content or connect content users to each other."[132] Judge Gould's dissent agreed with Judge Berzon's concurrence, arguing that Google "amplified and in part developed the terrorist message by encouraging similar views to be given to those already determined to be most susceptible to the ISIS cause."[133] Judge Gould argued that § 230 should not shield the defendant companies from liability for these activities.[134] Judge Gould also argued that the algorithms in question in *Gonzalez* are not neutral. He said that they may be "seemingly neutral," but in reality they are "a force to intensify and magnify a message."[135] Thus, both Judge Berzon and Judge Gould agreed that the internet companies in question should not be held liable for content merely published to their platforms and other activities that fall squarely within the role of a "publisher" defined under § 230, but that the activities of the

127. *See id.* at 892–93.
128. *Id.* at 895.
129. *Id.*
130. *Id.*
131. *Id.* at 913 (Berzon, J., concurring).
132. *Id.*
133. *Id.* at 922 (Gould, J., concurring in part and dissenting in part).
134. *See id.*
135. *Id.* at 921 (Gould, J., concurring in part and dissenting in part).

recommendation algorithms go far beyond normal publishing activities and therefore should not receive § 230 immunity.[136]

C. RECENT SUPREME COURT CASES: *TWITTER V. TAAMNEH* (2023) AND *MOODY V. NETCHOICE* (2024)

The Supreme Court has recently characterized recommendation algorithms in two cases outside of the § 230 context.[137] It is important to have a brief understanding of these cases, however, because lower courts have started to use at least the *Moody* opinion's characterization of recommendation algorithms to question the extent of § 230 immunity.[138]

In *Twitter v. Taamneh*, the Supreme Court collapsed the issues presented in *Gonzalez* with the issues presented in *Taamneh* as they both involved social media platforms sued for allegedly aiding and abetting acts of terrorism.[139] In *Taamneh*, the Court ruled in favor of the social media companies, holding that they did not aid and abet terrorists under 18 U.S.C. § 2333, which provides a cause of action to plaintiffs injured by "an act of international terrorism."[140] The difference between *Taamneh* and *Gonzalez* is that the former did not raise § 230 concerns.[141] Despite the Court avoiding the § 230 concerns in its *Taamneh* decision, Justice Thomas briefly discussed recommendation

136. *See id.* at 913, 922 (Berzon, J., concurring; Gould, J., concurring in part and dissenting in part).

137. *See generally* Twitter, Inc. v. Taamneh, 598 U.S. 471 (2023); Moody v. NetChoice, LLC, 144 S. Ct. 2383 (2024).

138. *See* Anderson v. TikTok, Inc., 116 F.4th 180, 183–84 (3d Cir. 2024).

139. *Twitter, Inc. v. Taamneh*, *supra* note 121.

140. *See generally Taamneh*, 598 U.S. at 506; 18 U.S.C. § 2333(d)(2).

141. Before the Supreme Court filed its decision in *Taamneh* and *Gonzalez*, many believed *Gonzalez* would be the first time the Supreme Court would address the scope of § 230 and, specifically, if immunity extends to recommendation algorithms. *Google v. Gonzales LLC,* ACLU (May 18, 2023), https://www.aclu.org/cases/google-v-gonzalez-llc. Some commentators agreed with the Court's decision to avoid the § 230 issue. Aaron Mackey, *The Internet Dodges Censorship by the Supreme Court*, ELEC. FRONTIER FOUND. (May 18, 2023), https://www.eff.org/deeplinks/2023/05/internet-dodges-censorship-supreme-court. Justice Kagan herself noted that the Justices are "not, like, the nine greatest experts on the internet." Vittoria Elliott & Dell Cameron, *The US Supreme Court Doesn't Understand the Internet*, WIRED (Feb. 22, 2023), https://www.wired.com/story/the-supreme-court-section-230-the-internet/. In ruling the way they did, the Court avoided making an "erroneous judgment on a technical question with far-reaching consequences" and left to Congress the job of defining the scope of § 230 if it so chooses. *Twitter, Inc. v. Taamneh*, *supra* note 121. Others, however, wanted the Court to finally address § 230 and provide some workable guidelines for lower courts on how to address claims allegedly barred by § 230. *Id.* As one scholar noted that "[g]iven the ubiquity of algorithms and their importance to the operation of many websites, less guidance on the question means that lower courts and social media platforms will continue to wrestle with uncertainties about legal liability." *Id.*

algorithms in the context of torts in his opinion.[142] Justice Thomas disagreed with the plaintiffs' assertion that recommendation algorithms "go beyond passive aid and constitute active, substantial assistance."[143] Instead, he wrote, "algorithms appear agnostic as to the nature of the content, matching any content . . . with any user who is more likely to view that content. The fact that these algorithms matched some ISIS content with some users thus does not convert defendants' passive assistance into active abetting."[144] While the Court did not address § 230 in *Taamneh*, its understanding of what an algorithm is, even if not explicitly connected to the § 230 issue, could have implications for future § 230 litigation. As Daphne Keller, the Director of Platform Regulation at Stanford's Cyber Policy Center has said, "[the Court's] broad statements about platform passivity will give future litigants a lot of jurisprudential spaghetti to throw at the wall."[145]

In *Moody v. NetChoice*, the Court vacated and remanded two judgements from the Eleventh and Fifth Circuits that challenged the constitutionality of two statutes that aimed to regulate large social media companies.[146] The Texas law in question required, among other things, that large social media companies make certain disclosures about the content they remove and establish complaint procedures for those who had content removed from the platform.[147] The Florida law was similar in that it established a violation when social media companies removed political candidates from their platforms and mandated requirements for when social media companies restrict users' speech.[148] Plaintiffs challenged both laws on First Amendment grounds. The Fifth Circuit and Eleventh Circuit came to opposite conclusions about the constitutionality of the laws. The Supreme Court vacated and remanded both judgements because neither circuit adequately analyzed the facial First Amendment challenge to the statutes.[149]

However, the Court took an opportunity in *Moody* to establish that content moderation policies are platforms' expressive content and are therefore protected under the First Amendment.[150] In doing so, the Court discussed how

142. *Taamneh*, 598 U.S. at 499.

143. *Id.*

144. *Id.*

145. Daphne Keller, *Carriage and Removal Requirements for Internet Platforms: What* Taamneh *Tells Us*, 4 J. FREE SPEECH L. 87, 93 (2023).

146. *See Moody*, 603 U.S. at 745.

147. *See id.* at 717–18.

148. *See id.*

149. *See id.* at 734–35.

150. *See id.* at 744.

algorithms factor into content moderation.[151] The Court was very careful in its analysis of algorithms and made clear that there are multiple types of algorithms. For example, the Court held that algorithms guided by platform standards establishing the type of permissible content are expressive content.[152] In one footnote, the Court made clear that it "do[es] not deal here with feeds whose algorithms respond solely to how users act online—giving them the content they appear to want, without any regard to independent content standards."[153] In her concurrence, Justice Barrett stated that algorithms that "present[] automatically to each user whatever the algorithm thinks the user will like," might not receive the same First Amendment protections as those algorithms guided by platform standards and policies.[154]

D. Anderson v. TikTok (2024)

A Third Circuit decision that came down in August 2024 has made it clear that the issue of § 230 immunity and its relationship to recommendation algorithms is not going away. In *Anderson*, the Third Circuit examined whether § 230 barred state claims against TikTok's For You Page for promoting content to a young girl that resulted in her accidentally killing herself.[155] The Third Circuit held that § 230 did not bar these claims.[156] The case centered on a ten-year-old girl, Nylah Anderson, who saw videos on TikTok's personally curated For You Page that depicted what is known as the "Blackout Challenge."[157] The viral challenge encouraged users to post videos of themselves taking part in self-asphyxiation. Anderson's mother sued TikTok for violations of state law after Anderson attempted the challenge and unintentionally hung herself.[158]

Instead of using the ubiquitous *Barnes* test to examine TikTok's For You Page under § 230, the Third Circuit did something unexpected and instead relied on the Supreme Court's characterization of algorithms in *Moody* to make its § 230 determination.[159] The Third Circuit determined that TikTok could not invoke § 230 immunity against the claims because TikTok's For You Page algorithm is TikTok's own expressive activity.[160] The Third Circuit held that

151. *See id.* at 734–35.
152. *See id.* at 735–38.
153. *See id.* at 736 n.5.
154. *Id.* at 746 (Barrett, J., concurring).
155. *See Anderson*, 116 F.4th at 181.
156. *Id.*
157. *Id.*
158. *Id.*
159. *See id.* at 183.
160. *Id.* at 184.

§ 230 immunity only extends to information "provided by another" and not a platform's own expressive activity.[161]

E. WHERE COURTS STAND NOW

With the Third Circuit's opinion in *Anderson*, there is now a circuit split with how appellate courts interpret § 230 applying to recommendation algorithms. The Third Circuit held that § 230 does not bar a plaintiff's claim that a recommendation algorithm played a role in her daughter's death because TikTok's recommendation algorithm can be considered the platform's own content.[162] This stands in stark contrast to the decisions in *Force* and *Gonzalez*, which are still precedent in the Second and Ninth Circuits.

Many criticized the Third Circuit's reasoning in *Anderson*, pointing out that applying *Moody* was faulty because *Moody* dealt with First Amendment issues and therefore was an inappropriate precedent to apply to a § 230 case.[163] TikTok petitioned the Third Circuit for a rehearing and a rehearing en banc.[164] The Third Circuit has denied this petition.[165] It is not yet known whether the Supreme Court will grant certiorari in this case. However, this circuit split indicates a need for the Court to finally settle the issue of how lower courts should analyze algorithms under § 230.[166]

---

161. *See id.* at 183–84.

162. *Id.* at 184.

163. Ryan Calo, *Courts Should Hold Social Media Accountable—But Not By Ignoring Federal Law*, HARV. L. REV. (Sep. 10, 2024), https://harvardlawreview.org/blog/2024/09/courts-should-hold-social-media-accountable-but-not-by-ignoring-federal-law/; Eric Goldman, *Bonkers Opinion Repeals Section 230 In the Third Circuit*—Anderson v. TikTok, TECH. & MKTG. L. BLOG (Aug. 29, 2024), https://blog.ericgoldman.org/archives/2024/08/bonkers-opinion-repeals-section-230-in-the-third-circuit-anderson-v-tiktok.html.

164. Emily Field, *TikTok Won't Get 3rd Circ. Rehearing of Section 230 Ruling*, LAW360 (Oct. 24, 2024), https://www.law360.com/articles/2251176.

165. *Id.*

166. In February 2025, the circuit split over recommendation algorithms deepened when the Fourth Circuit held that § 230 barred a plaintiff's state tort law claims against Meta (Facebook's parent company) that sought to hold Meta liable for the way it prioritizes content to users of its platform. M.P. by and through Pinckney v. Meta Platforms Inc., 127 F.4th 516, 521 (4th Cir. 2025). The plaintiff's father had been killed by Dylann Roof in a mass shooting in a South Carolina church. *Id.* Plaintiff alleged Meta's recommendation algorithms were in part to blame for radicalizing Roof because the company allows "racist, harmful content to appear on its platform and directs that content to likely receptive users to maximize Facebook's profits." *Id.* at 525. The Fourth Circuit noted that there was no meaningful disagreement between the parties on the first and third prongs of the *Barnes* test. *Id.* at 524. However, the Fourth Circuit found that Facebook served as a publisher under the second prong of the *Barnes* test despite the fact that Facebook boosts certain content for the sake of raising engagement. *Id.* at 526. The Fourth Circuit said that using an algorithm to maximize engagement and profits "does not change the underlying nature of the act that it is performing.

IV. CHALLENGING THE COURTS' CURRENT APPROACH

While Part III described how appellate courts and the Supreme Court have examined algorithms both inside and outside the context of § 230, Part IV will first explain how the appellate courts' approach thus far in performing a *Barnes* test analysis on algorithms has been overbroad and flawed. The second component of Part IV will then propose a new, individualized, and fact-intensive approach to assessing algorithms under § 230. Under this new approach, any analysis of algorithms under Prongs Two and Three of the *Barnes* test should examine each algorithm on its own, separate from the other algorithms used within the same company or across companies. Part IV will then apply this narrow, individual tools analysis to the *Anderson* case to show how this proposed approach could lead to a similar outcome in that case without the Third Circuit's use of ill-fitting precedent. Part IV will lastly tackle some challenges to implementing this new approach and offer solutions.

A. APPELLATE COURTS' CURRENT APPROACH TO ANALYZING ALGORITHMS UNDER THE *BARNES* TEST SHOULD BE RECONSIDERED

Section IV.A will discuss how many social media platforms create and maintain tools that do not serve publishing functions, which is an important consideration for a Prong Two analysis under the *Barnes* test. Similarly, Section IV.A will also examine how different algorithms within and across social media platforms can differ from one another, which is critical for a Prong Three analysis under the *Barnes* test. Section IV.A will then suggest that various courts' methods in analyzing algorithms have been overbroad, flawed, or both because the methods are seemingly based on the notion that social media platforms act as publishers in a general sense and that all algorithms are the same.

1. *Not All Activities of Social Media Platforms Mimic Traditional Publisher Functions, and Not All Algorithms Are the Same*

Many of the companies that are implicated in the court cases involving algorithms are massive entities that offer users and customers many different types of experiences and products.[167] There is no doubt that social media platforms can be considered publishers of third-party content. However, many

Decisions about whether and how to display certain information provided by third parties are traditional editorial functions of publishers, notwithstanding the various methods they use in performing that task." *Id.*

167. *See, e.g.*, GOOGLE, https://about.google/intl/ALL_us/products/ (last visited Nov. 14, 2024); *see* META, https://business.meta.com/ (last visited Nov. 14, 2024); META, https://www.meta.com/ (last visited Nov. 14, 2024).

of these companies also engage in a wide range of activities that have nothing to do with publishing. For example, a quick look at the list of Google's products will immediately present tools that are used primarily for data storage, like One, or data organization, like Google Sheets.[168] Likewise, Meta is developing what it calls the Metaverse, a new artificial world in which people from around the physical world can be connected in a virtual world.[169] Both companies have also built and continue to develop their own generative artificial intelligence tools and platforms.[170] These newer products, or tools, will seemingly be entirely different than many of the tools for which Meta is currently known like direct messaging over WhatsApp or buying and selling on Facebook Marketplace. While this may seem obvious to anyone who uses the internet today, it is important, for the purposes of this Note and any *Barnes* Prong Two analysis, to highlight the wide variety of tools that can exist on any given platform.

In addition to social media platforms offering many different types of tools for many different types of functions, each individual platform uses different types of algorithms for different purposes across its internal tools and systems.[171] Technically speaking, recommendation systems or algorithms can be based on a variety of different machine-learning models like primary ranking models, peripheral ranking models, and auxiliary models.[172] Each of these models serves different functions. Primary ranking models suggest relevant content to users.[173] Peripheral ranking models suggest accounts to follow or surface advertisements.[174] Auxiliary models generally perform content moderation tasks.[175] In addition to using machine models to develop recommendation systems, companies also apply manual, rule-based models to the machine-modeled recommendation systems to help refine how content is

168. *See* GOOGLE, *supra* note 167.

169. *See* Eric Ravenscraft, *What Is the Metaverse, Exactly?*, WIRED (June 15, 2023), https://www.wired.com/story/what-is-the-metaverse/; Mike Isaac, *Meta Unveils New Smart Glasses and Headsets in Pursuit of the Metaverse*, N.Y. TIMES (Sep. 25, 2024), https://www.nytimes.com/2024/09/25/technology/meta-products-artificial-intelligence.html.

169. *See generally* META AI, www.meta.ai (last visited Oct. 2, 2025); META GOOGLE GEMINI, gemini.google.com (last visited Oct. 2, 2025).

171. Kristian Lum & Tomo Lazovich, *The Myth of The Algorithm: A System-Level View of Algorithmic Amplification*, KNIGHT FIRST AMEND. INST. AT COLUM. U. (Sep. 13, 2023), https://knightcolumbia.org/content/the-myth-of-the-algorithm-a-system-level-view-of-algorithmic-amplification.

172. *See id.*

173. *See id.*

174. *See id.*

175. *See id.*

displayed to the user in a way that aligns with different business goals.[176] For example, engineers will manually change algorithms so that certain content does not appear next to certain brands' advertisements or to make sure that users' feeds are not too repetitive.[177]

Furthermore, different algorithms can have different objectives and purposes across a platform's different tools. For example, some algorithms prioritize exploiting content, like Google search, while others are built more for exploration, like Instagram's Explore tab.[178] Some algorithms try to accomplish both goals at the same time, which is what TikTok's primary recommender system, the For You Page, does.[179]

Additionally, there can even be different algorithms with different objectives that fuel the same recommendation algorithm or system. Engineering teams with varying goals can and do apply different algorithms to the same recommendation system, like Facebook's newsfeed.[180] Facebook uses hundreds if not thousands of algorithms to rank content in its newsfeed alone.[181] Some of those algorithms are designed with recommending content in mind and are therefore based on data gathered from user inputs and preferences, while other algorithms are built to serve as detection tools for "bad content" that the company wants to make sure is demoted in users' feeds.[182]

2. *Appellate Courts Overgeneralize Platforms' Publisher Status and Ignore Important Differences Among Algorithms, Leading to Flawed Analyses Under the* Barnes *and Material Contribution Tests*

Most appellate court cases that have examined algorithms have used an overbroad and flawed approach that has created an idea that extending § 230 immunity to algorithms must be an all-or-nothing inquiry. This approach is flawed because it does not consider the different functions platforms have beyond that of traditional publishing or the differences among algorithms. The all-or-nothing approach, therefore, likely extends § 230 immunity past where it should be extended under the established *Barnes* and material contribution tests.

---

176. *See id.*

177. *See id.*

178. *See* Jonathan Stray, Luke Thorburn & Priyanjana Bengani, *What's the Difference Between Search and Recommendation?*, TECH POL'Y PRESS (Oct. 16, 2023), https://www.techpolicy.press/whats-the-difference-between-search-and-recommendation/.

179. *See id.*

180. *See* Hao, *supra* note 92.

181. *Id.*

182. *Id.*

In *Force* and *Gonzalez*, the Second and Ninth Circuits examined social media platforms as a whole when determining their roles as publishers under Prong Two of the *Barnes* test.[183] Even when it addressed how "Facebook's algorithm" could place it outside the role of a publisher, the Second Circuit suggested that Facebook was either a publisher or not for the purposes of Prong Two. However, categorizing all the entire Facebook product experience as a publisher is overly simplistic and creates a situation in which the entire Facebook application is conflated with one out of many of its specific tools. Facebook, or Meta, offers dozens, if not hundreds, of different tools. A user can post on their own page, send private messages to friends, play games, buy goods on the marketplace, plan an event, join groups relevant to their interests, and peruse their "newsfeed."[184] The better question is whether or not Facebook's individual tools, like its newsfeed or instant messaging service, serve publishing functions, not whether Facebook as a whole is a publisher.

Additionally, in *Force* and *Gonzalez*, the Second and Ninth Circuits overgeneralized the way in which Facebook's and Google's algorithms work. For example, while the *Force* opinion noted that there are different algorithms used across the platform, much of the language and reasoning of the opinion suggested that the algorithms use similar inputs of data and work in fundamentally the same way.[185]

However, there is evidence that Facebook's various algorithms can differ widely from one another. Based on interviews with Facebook executives, current and former employees, and experts, an MIT Technology Review Investigation found that "Facebook decides how to target ads and rank content based on hundreds, perhaps thousands, of algorithms."[186] The report also found that engineers on different teams with different business objectives "develop and add their own machine-learning models into the mix, based on their team's objectives."[187] Furthermore, multiple teams across Facebook contribute to just its newsfeed recommendation system.[188] This creates a situation in which one system can be so "complex and unwieldy that no one can keep track anymore of all of its different components."[189] This description

---

183. *See Force*, 934 F.3d at 65; *Gonzalez*, 2 F.4th at 892.

184. *See generally* FACEBOOK, www.facebook.com (last visited Dec. 18, 2024).

185. *Force*, 934 F.3d at 70.

186. Hao, *supra* note 92; *see* Karen Hao, *How Facebook Got Addicted to Spreading Misinformation*, MIT TECH. REV. (Mar. 11, 2021), https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/.

187. Hao, *supra* note 92.

188. *Id.*

189. *Id.*

of Facebook's algorithms is a far cry from the Second Circuit's characterization of Facebook's algorithms in *Force*.[190]

The Ninth Circuit, in turn, compared Google's algorithms to search engines—which are completely different tools that serve a different purpose than a recommendation system—and other algorithms at issue in earlier cases, suggesting Google's algorithms function the same way as these other tools or algorithms.[191] The Ninth Circuit used the similarities it found between search engines and recommendation algorithms to argue that the plaintiffs' complaints fail Prong Three of the *Barnes* test.[192] Thus, the Ninth Circuit implied that search engines and recommendation systems are the same under Prong Three of *Barnes*.[193] This is a flawed analysis because while both tools are built using algorithms, there is ample evidence to show that search engines are different than recommendation algorithms in function, build, and purpose.[194]

The Third Circuit's opinion in *Anderson* arguably moved closer to singling out individual recommendation systems than the previous decisions had. The Third Circuit recognized TikTok's For You Page as a singular tool across the opinion. The Third Circuit did this in part by noting the particular features of the algorithm behind TikTok's For You Page. These features included "curat[ing] and recommend[ing] a tailored compilation of videos . . . based on a variety of factors, including the user's age and other demographics, online interactions, and other metadata."[195] On its face, the Third Circuit's description of TikTok's For You Page is similar to the Second Circuit's description of Facebook's algorithms, but the key difference in *Anderson* is that the Third Circuit examined the For You Page on its own without implicating multiple tools in one overbroad analysis.[196] The Third Circuit occasionally used somewhat broad language. For example, it uses the term "TikTok's algorithm" many times when discussing the For You Page. However, it is clear by the way the opinion is written that the Third Circuit was consistently discussing the For You Page algorithm specifically without suggesting the For You Page is

190. *See Force*, 934 F.3d at 70 ("The algorithms take the information provided by Facebook users and 'match' it to other users—again, materially unaltered—based on objective factors applicable to any content, whether it concerns soccer, Picasso, or plumbers. Merely arranging and displaying others' content to users of Facebook through such algorithms—even if the content is not actively sought by those users—is not enough to hold Facebook responsible as the 'develop[er]' or 'creat[or]' of that content. *See, e.g.*, *Marshall's Locksmith*, 925 F.3d at 1269–71; *Roommates.Com*, 521 F.3d at 1169–70.").

191. *See Gonzalez*, 2 F.4th at 895.

192. *See id.* at 896.

193. *See* Stray, *supra* note 178.

194. *See generally id.*

195. *Anderson*, 116 F.4th at 182.

196. *See generally Force*, 934 F.3d at 69–70; *Anderson*, 116 F.4th at 181.

similar or dissimilar to other algorithms within TikTok or across other platforms.

However, the Third Circuit's *Anderson* decision is flawed for other reasons. It relied on and mischaracterized the Supreme Court's decision in *Moody*.[197] The *Moody* decision recognized that different types of algorithms serve different functions even within one platform.[198] The Court made it clear that it was only looking at algorithms that are guided by the platform's content standards and policies.[199] The Court made a point to suggest that the content-moderation algorithms with which they were most concerned are not necessarily the same as algorithms that focus mostly on presenting relevant content to users like that which is at issue in *Anderson*.[200] Therefore, the Third Circuit applied the Court's reasoning in *Moody* to the exact type of algorithm the Court said was not implicated in its analysis in the *Moody* opinion, effectively mischaracterizing and watering down the Supreme Court's nuanced assessment of algorithms in *Moody*.

3. *The Supreme Court Also Ignored Differences Among Algorithms in* Taamneh *but Acknowledged Them in* Moody

While the Supreme Court has not yet addressed whether § 230 extends to algorithms, they recently used a broad, sweeping approach to characterize algorithms in *Taamneh* but seemingly showed a more nuanced understanding of algorithms in *Moody* as discussed*, supra*, Section III.C.

In *Taamneh*, the Court described algorithms as "passive" when establishing whether social media platforms played a role in aiding and abetting a terrorist attack and could therefore be held liable under federal law.[201] This characterization of algorithms is overbroad and seems to suggest that all algorithms, regardless of the platform, have this "passive" quality. However, in *Moody*, the Court seemed to take a different approach to characterizing algorithms than in *Taamneh* by suggesting that different types of algorithms may be subject to different legal protections.[202] For example, the Court was only willing to grant First Amendment rights to platforms' algorithms that were designed with content policies in mind.[203] The Court suggested that they

197. *See generally Anderson*, 116 F.4th at 183–84.
198. *See Moody*, 603 U.S. at 735–38.
199. *Id.*
200. *Id.* at 746 (Barrett, J., concurring).
201. *Taamneh*, 598 U.S. at 499.
202. *See generally Moody*, 603 U.S. at 735.
203. *Id.*

would not address whether these same rights would be extended to other algorithms the platform may use for other purposes.[204]

It is unclear why the Supreme Court characterized algorithms in such different ways in the *Taamneh* and *Moody* decisions. It is likely that the Court did so because the cases themselves presented very different issues. *Taamneh* examined social media platforms' role in aiding and abetting terrorism, while *Moody* looked at social media companies' First Amendment rights in relation to their content moderation policies. The way the Court characterized algorithms in each decision likely had to do with supporting a desired outcome in each case.

Even though the Court addressed the nature of algorithms outside the § 230 context, its characterization of algorithms in *Moody* has already implicated a case that involves § 230: *Anderson*. If TikTok petitions for and the Court decides to grant certiorari in the *Anderson* case, the Court could correct its overbroad characterization of algorithms in *Taamneh* and continue down the path it started on in *Moody*. The Court should ultimately establish an analytical approach that examines each specific algorithm at issue in a case narrowly.

B. A Different Approach: A Narrow, Fact-Intensive Examination of Individual Algorithms Under Section 230

Section IV.B will propose a different approach than the overgeneralized ones most courts have taken when addressing social media platforms' algorithms. This new approach is called "the individual tools approach" and should be applied during an analysis of Prongs Two and Three of the *Barnes* test and the material contribution test. Section IV.B will then apply the proposed approach to *Anderson* and show how using this approach could result in a similar outcome without relying on *Moody*. Lastly, Section IV.B will examine the challenges in implementing this new approach and propose some solutions. Challenges include how plaintiffs might get past a motion to dismiss stage with limited evidence, the fact that machine-learning algorithms are black boxes, and general free speech concerns.

1. *Courts Should Focus on As Specific a Tool As Possible When Conducting an Analysis Under Prongs Two and Three of the* Barnes *Test*

As established, *supra*, in Section IV.A, many social media platforms serve multiple functions and provide many tools beyond ones that could be considered "publishing" tools. Under the individual tools approach, there is a difference between being a publisher and using tools that serve publishing

204. *See id.* at 736 n.5.

functions. The former suggests that a social media company can be considered a publisher in its entirety. The latter acknowledges the reality that companies may serve publishing functions through specific tools while also recognizing that many of these companies are not categorically publishers. Under this approach, companies won't be able to hide behind generalizations of their function in society to escape liability.

Under the individual tools approach, once the individual tool in question—whether that be an individual algorithm that is part of a larger recommendation system, an entire recommendation system itself, a search engine for users to explore content, an ads builder, a direct messaging system, etc.—has been identified, an analysis of Prong Two should then ask: is this specific tool functioning in a way that can be compared to traditional publishing?

Take Facebook's newsfeed, for example. As discussed, *supra*, Sections IV.A.1 and IV.A.2, it is a recommendation system that uses multiple algorithms to supply users with content in a way that is completely unique to that system. Facebook's parent company Meta also has, as discussed previously, a plethora of other tools that are separate from its newsfeed: some that use algorithms and some that do not and some that might behave similarly to a traditional publisher and some that unquestionably do not.[205] Under the new approach, the question for the second prong of the *Barnes* test can focus on whether the entire recommendation system or even just one of the specific algorithms that creates that larger system serves a traditional publishing function, not whether Meta in its entirety is comparable to a traditional publisher.

The analysis for whether an individual algorithm or system of algorithms should be considered to serve publishing functions can then mimic the analysis of whether the platform as a whole should be considered a publisher. This analysis was introduced in *Zeran* and discussed in subsequent appellate decisions.[206] In *Zeran*, the Fourth Circuit said § 230 precludes claims that originate from "traditional editorial functions . . . such as such as deciding whether to publish, withdraw, postpone, or alter content."[207] The Second Circuit in *Force* said that it and other courts have examined the ordinary meaning of the term "'publisher'" in § 230(c)(1), which is "'one that makes

205. *See* META, https://business.meta.com/ (last visited Nov. 14, 2024); META, https://www.meta.com/ (last visited Nov. 14, 2024).

206. *See Force*, 934 F.3d at 64; *Gonzalez*, 2 F.4th at 892–93.

207. *Zeran*, 129 F.3d at 330.

public,'"[208] "'the reproducer of a work intended for public consumption,'"[209] and "'one whose business is publication.'"[210] Drawing on the opinions in *Roommates.com* and *Barnes*, the Ninth Circuit largely mimicked the *Zeran* approach in examining the publisher question in *Gonzalez*, stating that publishing includes "'reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content.'"[211]

Courts can ask several questions to determine whether the individual tool in question is serving a publishing function based on the Second and Ninth Circuits' understanding of what it means to be a publisher. The example of Facebook's newsfeed is again illustrative. The purpose of that system, on its face, is to recommend and suggest content to users based on user signals, like previous content they have liked.[212] A court could first ask whether that activity mimics that of a traditional publisher. While this arguably goes beyond the mere function of "making something public," it could be possible for a court to decide that recommending content to users fits more into the "'reviewing, editing, and deciding whether to publish'" function.[213]

The next question might become: Do traditional publishers actively promote biased content to change user's behavior and beliefs and to increase the amount of time users spend on the platform? The answer to this question is currently unclear and might be difficult to ascertain without plaintiffs being able to gather more information during the pleading stage.[214] It is hard to imagine any traditional publisher behaving in such an extreme fashion, but that is an inquiry the courts can make with sufficient information. For example, studies have shown that Facebook's newsfeed takes some actions in how it organizes content that could be considered to go beyond the role of a traditional publisher.[215] Courts will likely need evidentiary support about how

---

208. *Force*, 934 F.3d at 65 (citing Klayman v. Zuckerberg, 753 F.3d 1354, 1359 (D.C. Cir. 2014)).

209. *Force*, 934 F.3d at 65 (citing Fed. Trade Comm'n v. LeadClick Media, LLC, 838 F.3d 158, 175 (2d Cir. 2016)).

210. *Id.*

211. *Gonzalez*, 2 F.4th at 892 (quoting *Barnes*, 570 F.3d at 1102).

212. *See* Sam Lauron, *2025 Facebook Algorithm: Tips and Expert Secrets to Succeed*, HOOTSUITE (Feb. 3, 2025), https://blog.hootsuite.com/facebook-algorithm/.

213. *Gonzalez*, 2 F.4th at 892.

214. Most of the cases in which a § 230 claim does not survive the *Barnes* test are decided on a motion to dismiss. How to survive a motion to dismiss will be discussed later in this Note.

215. *See* Huo Jingnan & Shannon Bond, *New Study Shows Just How Facebook's Algorithm Shapes Conservative and Liberal Bubbles*, NPR (July 27, 2023), https://www.npr.org/2023/07/27/1190383104/new-study-shows-just-how-facebooks-algorithm-shapes-conservative-and-liberal-bub; *see also* Will Oremus, Chris Alcantara, Jeremy B. Merrill & Artur Galocha, *How*

individual algorithms work to draw a line somewhere between when an algorithm functions similarly to a traditional publisher and when it does not. While that line is not yet known,[216] it will be a lot easier for courts to establish that line if they are able to work off clear evidence about how individual algorithms work and subsequently single out each individual algorithm in their Prong Two analysis. Once each algorithm is singled out, courts can decide which algorithms pass a Prong Two analysis and which ones fail that same analysis.

Similar to singling out individual tools in a Prong Two analysis, courts should also conduct fact-specific determinations about each algorithm in question during the Prong Three analysis in order to avoid making sweeping generalizations about all algorithms. As stated earlier, while algorithms share many similarities, there are ample differences among them across different platforms, within the same platform, and even within the same recommendation system.[217] Under this new approach, once an individual algorithm has been identified and isolated, the question courts need to answer under Prong Three and the material contribution test is if that algorithm developed, co-developed, or materially contributed to the offending content. Taking this approach will protect the integrity of § 230 and avoid extending liability or immunity further than necessary. In other words, if one algorithm is found to have failed Prong Three of the *Barnes* test, other algorithms separate from or even within the same recommendation system will not be implicated and can presumably continue to function as they always have.

Take X (formerly "Twitter")'s "For you" tab as an illustrative example. It has been reported that current X owner, Elon Musk, asked engineers to promote his content so that it was higher in users' feeds shortly after he took

Facebook Shapes Your Feed, WASH. POST (Oct. 23, 2021), https://www.washingtonpost.com/technology/interactive/2021/how-facebook-algorithm-works/.

216. Even in Anderson, the court did not address the publisher issue, instead conducting essentially a Prong Three analysis. *See Anderson*, 116 F.4th at 183–84.

217. *See generally* Akos Lada, *How Does New Feed Predict What You Want to See?*, FACEBOOK NEWSROOM (Jan. 26, 2021), https://about.fb.com/news/2021/01/how-does-news-feed-predict-what-you-want-to-see; *see* Nima Noorshams, Saurabh Verma & Aude Hofleitner, *Leveraging Online Social Interactions for Enhancing Integrity at Facebook*, META RSCH. BLOG (Aug. 26, 2022), https://research.facebook.com/blog/2020/8/leveraging-online-social-interactions-for-enhancing-integrity-at-facebook/; *The Facebook Algorithm Explained*, BRANDWATCH (May 7, 2021), https://www.brandwatch.com/blog/the-facebook-algorithm-explained/; *Explained: The Algorithms that Run Facebook*, ECON. TIMES (Oct. 26, 2021), https://economictimes.indiatimes.com/tech/trendspotting/explained-the-algorithms-that-run-facebook/articleshow/87282136.cms?from=mdr.

over the company.[218] If a court were to examine X's "For you" recommendation system under Musk's influence, it is likely that they could find that the "For you" tab does not pass Prong Three. This is because X's engineers arguably co-developed and possibly even materially contributed to the content published on the "For you" tab by actively promoting Elon Musk's content to all users regardless of whether they wanted to follow him or not. If a court were to make this determination, the algorithm responsible for promoting Elon Musk's post would not receive § 230 immunity. However, the other algorithms fueling the "For you" page, like those which show users content related to their proven interests, could remain untouched by that decision, as would all other algorithms on X and other platforms unless separately challenged and tested under the individual tools approach. In this way, the individual, fact-intensive approach can make it so that § 230 immunity only extends to as narrow a group of algorithms as is absolutely necessary under the law without implicating every algorithm or system of algorithms that exist.

In the cases discussed, *supra*, in Parts III and IV of this Note, neither plaintiffs nor defendants have argued that courts should take this more individualized approach when analyzing algorithms. Plaintiffs' claims tend to overgeneralize algorithms when challenging their status under the last two prongs of the *Barnes* test, and defendants tend to respond in kind. This is likely due to a lack of available evidence at the pleading stage. The closest a court or party has come to suggesting a more individualized approach to examining algorithms comes from Chief Judge Katzmann of the Second Circuit in the *Force* dissent.[219] He argued that precedent does not suggest that publishers should be immune under § 230 for every activity in which they engage.[220] He said, "Facebook may be immune under the CDA from plaintiffs' challenge to its allowance of Hamas accounts, since Facebook acts solely as the publisher of the Hamas users' content. That does not mean, though, that it is also immune when it conducts statistical analyses of that information and delivers a message based on those analyses."[221]

If courts were to use the individual tools approach, the outcome may be that § 230 immunity is applied appropriately to protect the parts of the internet it was intended to protect while holding companies liable for conduct that

218. Faiz Siddiqui & Jeremy B. Merrill, *Elon Musk Reinvents Twitter for the Benefit of a Power User: Himself*, WASH. POST (Feb. 16, 2023), https://www.washingtonpost.com/technology/2023/02/16/elon-musk-twitter/.

219. *See generally Force*, 934 F.3d (Katzmann, C.J., concurring in part and dissenting in part).

220. *Force*, 934 F.3d at 81 (Katzmann, C.J., concurring in part and dissenting in part).

221. *Id.* at 83 (Katzmann, C.J., concurring in part and dissenting in part).

surpasses what § 230 seemingly meant to protect. With this narrower, fact-intensive approach, courts can decide about whether a specific recommendation system or an individual algorithm that is part of that larger system is subject to § 230 without making a judgement about whether every single recommendation system, algorithm, search engine, or any other type of tool is subject to the same immunity or liability. This would benefit both plaintiffs and defendants because plaintiffs would likely receive damages for harms caused by tools that should not be protected by § 230, while defendants would only be held liable for as small a portion of their technology as necessary under the law.

2. *Applying the Individual Tools Approach to* Anderson

As discussed, *supra*, in Section III.D, the Third Circuit in *Anderson* decided that TikTok's For You Page did not qualify for § 230 immunity because it determined that the For You Page was TikTok's own "expressive activity" under *Moody*.[222] The Third Circuit did not complete a full *Barnes* test analysis in its opinion but rather focused on the plain language of the statute, which states that § 230 only immunizes information "'provided by another.'"[223] That analysis is essentially a Prong Three analysis because Prong Three explicitly looks at who is providing the content in question, but the Third Circuit ultimately used a case that many find to be unrelated to the question at hand, *Moody*, to make its determination.[224]

Section IV.B.2 applies the individual tools approach under the *Barnes* test to analyze Anderson's claims against TikTok. Section IV.B.2 shows how this analysis would likely lead to a similar conclusion as was made by the Third Circuit without relying on caselaw that focuses on a different legal question or by making sweeping statements about how all algorithms function with § 230 as the Second and Ninth Circuits did in *Force* and *Gonazalez*.

a) Does TikTok's For You Page Function as a Traditional Publisher Under Prong Two of *Barnes*?

While the first inquiry in a *Barnes* test analysis is whether the defendant is an interactive computer provider, that question is rarely disputed, particularly in cases like *Anderson* that implicate a well-established social media company.[225] Accordingly, a *Barnes* analysis really begins at the second prong. Under the individual tools approach, the question is: does TikTok's For You Page, as an

222. *Anderson*, 116 F.4th at 183–84.
223. *Id.* at 184 (citing 47 U.S.C. § 230(c)(1)).
224. Calo, *supra* note 163; Goldman, *supra* note 163.
225. *See Force*, 934 F.3d at 69; *see also Gonzalez*, 2 F.4th at 891.

individual tool, function like a traditional publisher? The question is not the one many courts currently ask under Prong Two: Is TikTok a publisher as a whole?

To answer whether TikTok's For You Page functions as a traditional publisher, one first must consider whether the For You Page fits the definition: "'one that makes public,'"[226] "'the reproducer of a work intended for public consumption,'"[227] and "'one whose business is publication.'"[228] Much like Facebook's newsfeed discussed, *supra*, in Section IV.B.1, on its face TikTok's For You Page recommends new content to users based on previous content that they have engaged with. This function might fall into the definition of a traditional publisher. However, additional evidence might persuasively prove to the Supreme Court, if it grants certiorari in *Anderson*, that the For You Page goes beyond the function of a traditional publisher.

For example, there is evidence that TikTok's For You Page provides users with content the company believes that specific user wants to see, rather than content the user actually wants to see. In other words, the evidence suggests that the recommendation system promotes content that the platform thinks the user will watch.[229] While this behavior may not initially seem different to how other platforms' recommendation systems function, there is an important distinction to make between TikTok's For You Page and other potentially similar systems. In focusing on what the user will watch rather than what they have indicated they might want to watch, the algorithm can prey on people's vulnerabilities. For example, a teenager showing signs of depression may not want to watch depressing content, but when presented that content, they will likely watch it.[230] This is part of what is thought to make TikTok's For You Page distinct from other platforms' recommendation systems.[231] TikTok itself has seemingly recognized that this particular recommendation system can cause harm and has claimed to have attempted to put various safety measures

226. *Force* 934 F.3d at 65 (citing *Klayman*, 753 F.3d at 1359).
227. *Id.* (citing *LeadClick*, 838 F.3d at 175).
228. *Id.*
229. Sara Morrison, *TikTok Won't Stop Serving Me Horror and Death*, VOX (Oct. 26, 2022), https://www.vox.com/recode/2022/10/26/23423257/tiktok-for-you-page-algorithm.
230. *Id.*
231. Sara Morrison, *TikTok Is Confusing by Design*, VOX (July 5, 2023), https://www.vox.com/technology/23780112/tiktok-internet-design-algorithm-for-you-page-ux-ui.

in place to mitigate that harm.[232] However, evidence suggests that these efforts have been futile and unsuccessful.[233]

Given the evidence that exists about TikTok's For You Page, it is possible that a court would find that the specific recommendation system performs in a way that surpasses what a traditional publisher might do. For example, it is difficult to imagine a traditional publisher recognizing someone has a psychological disorder and providing that person content that makes that disorder worse for the sake of keeping them on their platform longer. In other words, if the facts surrounding how TikTok's algorithm is built suggest that it is purposefully designed to manipulate user behavior in a way that encourages people to watch content about self-harm, a court could use those facts about TikTok's algorithm to decide that it does not fall under § 230 protections. However, a court could decide the other way after a fact-intensive and individualized inquiry into how TikTok's For You Page operates. Under the individual tools approach, the publishing status will only apply to TikTok's For You Page and not to any of the other tools TikTok provides, like its "Following" or "Explore" tools, unless separately challenged and found to also fail the individual tools approach. The status will also not apply to other companies' recommendation systems unless it can be proved those systems also fail the newly proposed test.

b) Does TikTok's For You Page Develop, Co-develop, or Materially Contribute to the Offending Content Under Prong Three of *Barnes*?

The third and last inquiry made under the *Barnes* test is whether the algorithm that promoted the offending content developed, co-developed, or materially contributed to that content.[234] In this case the offending content is the Blackout Challenge videos that appeared on Nylah's For You Page.[235] An inquiry under the individual tools approach will only implicate the specific algorithm responsible for promoting these videos on Nylah's For You Page. To make its determination, a court will need to look at the facts surrounding the specific algorithm to make its determination.

Once again, it is possible that the Supreme Court, if it grants certiorari, could find that TikTok's For You Page does co-develop and materially contribute to the offending content. As discussed, *supra*, in Section IV.B.2.a,

232. Olivia Carville, *TikTok's Algorithm Keeps Pushing Suicide to Vulnerable Kids*, BLOOMBERG (Apr. 19, 2023), https://www.bloomberg.com/news/features/2023-04-20/tiktok-effects-on-mental-health-in-focus-after-teen-suicide.

233. *Id.*

234. *See Barnes*, 570 F.3d at 1100–01.

235. *See Anderson*, 116 F.4th at 181.

there is evidence to suggest that the For You Page provides users content that they never wanted to watch in the first place.[236] The For You Page instead promotes content that the user will likely watch, which can be very different than content users actually desire. Additionally, it has been suggested that TikTok's "'[a]lgorithmic processes . . . gamify harmful content'" to make it seem like entertainment to young people.[237] If a user does, in fact, watch novel and unexpected content, the algorithm will feed them more of that content. Thus, a strong argument could be made for considering this process to be one that materially contributes to the development of the offending content, even if TikTok itself did not create any Blackout Challenge videos.

There are also other possible outcomes under the individual tools analysis. First, it is entirely possible that one of the many algorithms that create the entire system of algorithms that is the For You Page is to blame for pushing nefarious content for the sake of increasing engagement. It is possible that a court would find that specific portion of the larger system is what makes the company liable for the offending content. Second, it is possible that a court could find that TikTok's For You Page does not in part develop the harmful content at all. Regardless of the decision a court might make regarding a Prong Three analysis of TikTok's For You Page, that decision will only apply to the specific, offending algorithm found responsible for promoting the Blackout Challenge on Nylah's For You Page under the individual tools approach.

3. *Potential Challenges or Concerns About the Individual Tools Approach*

a) Implementing the Individual Tools Approach Under the Federal Rules of Civil Procedure

One of the challenges courts will have in implementing the individual tools approach is that the rules of federal civil procedure make it very difficult for plaintiffs to gather enough evidence during the pleading stage to survive a motion to dismiss for failure to state a claim. As can be seen throughout the cases examined in this Note, plaintiffs often made broad accusations about the algorithms they sought to hold liable because the plaintiffs only had so much information available to them about how the algorithms. Furthermore, the *Barnes* and material contribution tests put the burden of proof on the plaintiff to prove that the defendant's conduct should not be barred by § 230.[238]

236. *See* Morrison, *supra* note 229.

237. Sally Weale, *Social Media Algorithms 'Amplifying Misogynistic Content'*, GUARDIAN (Feb. 5, 2024), https://www.theguardian.com/media/2024/feb/06/social-media-algorithms-amplifying-misogynistic-content; Cummins, *supra* note 3.

238. *See generally Force*, 934 F.3d; *Gonzalez*, 2 F.4th.

One solution to this problem is putting the burden on defendants instead of plaintiffs to prove that their algorithms pass the *Barnes* test. Another solution would be to allow plaintiffs to plead insufficient information under FRCP Rule 11(b)(3).[239] Rule 11(b) generally imposes certain requirements attorneys must meet in making any pleading, written motion, or other paper to avoid any pleading or other document that might cause "improper, frivolous, harassing, unnecessarily delayed, and unnecessarily expensive litigation."[240] Rule 11(b)(3) allows plaintiffs to make claims that "will likely have evidentiary support after a reasonable opportunity for further investigation or discovery."[241] While "[s]imply guessing or speculating that there may be a claim is not enough," plaintiffs can invoke 11(b)(3) during the pleading stage if they can "articulate at least some facts as to why it is reasonable to believe there is infringement."[242] In the context of gathering enough evidence to get past a motion to dismiss after a defendant has invoked a § 230 defense, plaintiffs would need to articulate some facts about the inner workings of an algorithm to show that the algorithm might not pass the *Barnes* test. If plaintiffs succeed with 11(b)(3) and can show that they have some facts that indicate an algorithm may not pass the *Barnes* test, they can then engage in further investigation or discovery to gather the evidence needed to prove their case.

b) Implementing the Individual Tools Approach Given the Black Box Methods of Machine-learning Algorithms

One argument social media companies are likely to make against the individual tool approach is that even if plaintiffs could gather more evidence about recommendation algorithms, many machine-learning algorithms are black boxes.[243] That is, no one understands why they work the way they do.[244] As experts note, "even those who design them, cannot understand how variables are being combined to make predictions. Even if one has a list of the input variables, black box predictive models can be such complicated functions of the variables that no human can understand how the variables are jointly related to each other to reach a final prediction."[245] Additionally, companies have a financial interest in creating black box models because it gives them a

239. FED R. CIV. P. 11(b)(3).

240. Elan Microelectronics v. Apple, No. C 09–01531, 2009 WL 2972374, at *3 (N.D. Cal. Sep. 14, 2009).

241. FED R. CIV. P. 11(b)(3).

242. *Elan*, No. C 09–01531, 2009 WL 2972374, at *4.

243. *See generally* Rudin, *supra* note 14.

244. *Id.*

245. *Id.*

competitive advantage over other companies given that no one can crack a particularly successful model, including the competitor.[246]

However, these same experts suggest that it is possible to design machine-learning models with interpretability constraints, which would mean that the models are built to be able to give people a better sense of how the system's predictions are actually made.[247] These models are technically equivalent to black box models but arguably much more ethical.[248]

For the individual tools analysis to ultimately be successful, a law that requires companies to build more interpretable tools might first be required.

c) Free Speech and Content Moderation Concerns If Any Company Is Found to Be Liable for Offensive Content Due to an Algorithm

Whenever § 230's scope is debated, one argument in favor of maintaining § 230's broad reach is that any effort to cut off platform immunity will both chill free speech and hamper content moderation policies.[249] The idea, in terms of chilling free speech, is that platforms will be afraid of being held liable for any content on their platforms and will end up censoring more content than is necessary in an effort to avoid lawsuits.[250] Another similar argument is that § 230 actually allows companies to moderate the content that exists on their platforms already without fear that they will be held liable for the decisions they make or for any content that falls through the gaps of their moderation practices and policies.[251]

While the free speech and content moderation concerns are something to take seriously when considering the scope of § 230, the individual tools approach makes it so platforms can adjust their recommendation algorithms to look something more like a traditional publisher or take a less active approach in prioritizing certain types of content without implicating all algorithms across the industry. For example, a company that is consistently being found liable for a recommendation system that fails either one or multiple prongs of the *Barnes* test could change or remove one of the many algorithms that comprise that recommendation system to make it so that it passes a *Barnes* test analysis. That same company could also switch to a system that posts content in a chronological order and from accounts that have only

246. *See id.*
247. *See id.*
248. *See id.*
249. Granick, *supra* note 22.
250. Draper, *supra* note 38.
251. Granick, *supra* note 22.

a few degrees of separation from accounts a user already follows. Changes like these would mean users are still allowed to post whatever speech they want. That speech may just find its way to other users in more organic ways than it currently does under certain algorithmic designs.[252]

Additionally, if it is important for business metrics to keep recommendation algorithms as they are, companies do have tools at their disposal to make their algorithms safer.[253] For example, companies take significant measures to prevent child pornography from appearing on their platforms. Those same measures can be taken to prevent other harmful or unlawful content from not only appearing but also being prioritized on people's feeds. In these ways, companies can still allow as much speech as they want on their platforms and continue to moderate content without fear of liability.

V. CONCLUSION

The internet has changed immensely since § 230 of the Communications Decency Act was enacted in 1996. In passing § 230, no one could have predicted the power of tools like recommendation systems and the individual algorithms that fuel them. The companies that wield these algorithms have a vested interest in continuing to use § 230 as a defense can to avoid liability, particularly when it comes to claims that implicate their most powerful tools. As discussed, many courts have handed social media platforms victories by suggesting that recommendation algorithms qualify for § 230 immunity under Prongs Two and Three of the *Barnes* test. The Third Circuit is the only court that has denied this immunity to a recommendation system. However, most of the decisions were based on an overbroad characterization of algorithms that take an all-or-nothing approach to applying § 230 to algorithms, setting unhelpful precedents for both plaintiffs and defendants.

If the Supreme Court grants certiorari for a case like *Anderson v. TikTok*, the Court has an opportunity to apply a more nuanced approach when examining how § 230 should apply to algorithms. It is what this Note has termed "the individual tools approach." Through examining each individual tool—whether that be looking at a recommendation system as a whole or one specific algorithm that helps run that larger system—on its own when doing a

252. *See generally* William J. Brady, Joshua Conrad Jackson, Björn Lindström & M. J. Crockett, *Algorithm-Mediated Social Learning in Online Social Networks*, 27 TRENDS IN COGNITIVE SCIS. 947 (2023).

253. Danielle Draper & Sabine Neschke, *The Pros and Cons of Social Media Algorithms*, BIPARTISAN POL'Y CTR. (Oct. 2023), https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2023/10/BPC_Tech-Algorithm-Tradeoffs_R01.pdf.

Barnes test analysis, § 230 immunity can be applied to the narrowest set of tools needed. This approach would protect the integrity of § 230 and would also protect defendants by making it so that similar tools across and within platforms would not be needlessly implicated. In turn, the tools that are found to fall outside the bounds of § 230 immunity could be appropriately held liable, benefitting plaintiffs and those who are at the mercy of social media companies' decisions.

Furthermore, the individual tools approach will be useful for courts analyzing how § 230 should be applied to even newer tools and technologies like those that are backed by generative AI. There has been much debate and speculation over how courts will interpret § 230 as it applies to AI-backed tools.[254] Under the individual tools approach, courts could single out AI tools from the other tools offered on social media platforms and assess how § 230 immunity relates to that specific, AI-backed tool without implicating other tools on the platform.

254. PETER J. BENSON & VALERIE C. BRANNON, CONG. RSCH. SERV., LSB11097, SECTION 230 IMMUNITY AND GENERATIVE ARTIFICIAL INTELLIGENCE 3 (2023); Noor Waheed, *Section 230 and Its Applicability to Generative AI: A Legal Analysis*, CTR. FOR DEMOCRACY & TECH. (Sep. 4, 2024), https://cdt.org/insights/section-230-and-its-applicability-to-generative-ai-a-legal-analysis/.