Washington Law Review Online

Volume 99 Article 1

2024

Breaking Algorithmic Immunity: Why Section 230 Immunity May Not Extend to Recommendation Algorithms

Max Del Real
University of Washington School of Law

Recommended Citation

Max Del Real, *Breaking Algorithmic Immunity: Why Section 230 Immunity May Not Extend to Recommendation Algorithms*, 99 WASH. L. REV. ONLINE 1 (2024).
Available at: https://digitalcommons.law.uw.edu/wlro/vol99/iss1/1

BREAKING ALGORITHMIC IMMUNITY: WHY SECTION 230 IMMUNITY MAY NOT EXTEND TO RECOMMENDATION ALGORITHMS

Max Del Real*

Abstract: In the mid-1990s, internet experiences were underwhelming by today's standards, despite the breakthrough technologies at their core. When a person logged on to the internet, they were met with a static experience. No matter who you were, where you were, or how you accessed a particular website, it rendered a consistent page. Today, internet experiences are personalized, dynamic, and vast—a far cry from the digital landscape of just a few decades ago. While today's internet is unrecognizable compared with its early predecessors, many of its governing laws remain materially unaltered. In particular, section 230 of the Communications Act, which passed in 1996, remains a critical element of the bedrock upon which the internet has flourished.

While the words of section 230's primary provisions remain unchanged, courts' applications have somewhat modernized to keep pace with technology. However, recommendation algorithms pose an especially tricky challenge for section 230 analyses. Initially, courts extended section 230 immunity to internet platforms for algorithmic recommendations of third-party information, but a growing cohort of circuit judges are questioning whether that treatment stretches the statute too far. Although the United States Supreme Court had an opportunity to weigh in through *Gonzalez v. Google*, that case's disposition ultimately left the issue open. This Comment dives deep into the current section 230 doctrine and examines its application to recommendation algorithms. While multiple theories have emerged that could successfully limit section 230 immunity's reach to recommendation algorithms, each will have distinct implications for the future of consumer technology. Regardless, there are multiple strategies that can feasibly negate section 230 immunity when the defendant has used recommendation algorithms.

INTRODUCTION

Since its passage in 1996, section 230 of the Communications Decency Act ("section 230") has shielded internet companies from liability in myriad cases. Although rooted in defamation law, defendants have successfully wielded section 230 in suits far afield from its origins. The statute's wide reach is commonly credited as a critical factor in the rapid

*J.D. Candidate, University of Washington School of Law, Class of 2024; B.S. 2011, M.S. 2012, Management Science and Engineering, Stanford University. Thank you to Professor Eric Schnapper and members of the University of Washington Tech Policy Lab for discussions that helped develop this topic. Thank you also to the *Washington Law Review Online* editors for the incredibly helpful feedback throughout the process.

and relatively frictionless growth of the internet because of its ability to reduce the risk of protracted litigations for budding startups and Silicon Valley behemoths alike.[1]

There are doubtless many aspects of the internet that would be unrecognizable without section 230. It has allowed free-flowing public expression, created space for social movements, and supercharged our ability to connect with friends and family.[2] If internet companies could not shield themselves from liability for defamatory statements made by third parties, it would have been nearly impossible to scale their platforms. And scaled platforms are an integral part of the modern internet.

Conversely, for people harmed by online content, that same shield may act as a barrier to justice and transparency. Because it is a form of immunity, internet companies invoke section 230 protection at the earliest stage of litigation.[3] As a result, when a judge grants immunity, the case is dismissed before trial, and the plaintiffs do not get a chance to illuminate the facts through discovery. Notably, when section 230 immunity is not granted, the defendant is not automatically liable—instead, the case proceeds to trial where a judge or jury will analyze the case and enter final judgment.

As technology progressed, section 230 provided aircover for tech companies, sometimes in circumstances that were undoubtedly outside the statute's original scope. One example, and the crux of this Comment, is section 230's application to recommendation algorithms. In broad terms, internet services use recommendation algorithms to personalize content for each user. For platforms with more information than users could conceivably consume, recommendation algorithms help identify the content with which users will most likely engage.[4] These algorithms have

[1] *See generally* JEFFREY KOSSEFF, THE 26 WORDS THAT CREATED THE INTERNET 3–4 (2019) ("Section 230 created the legal and social framework for the Internet we know today: the Internet that relies on content created not only by large companies. . . . Without Section 230, companies could be sued for their users' blog posts, social media ramblings, or homemade online videos. The mere prospect of such lawsuits would force websites and online service providers to reduce or entirely prohibit user-generated content. The Internet would be little more than an electronic version of a traditional newspaper or TV station, with all the words, pictures, and videos provided by a company and little interaction among users."); *see also* Gregory M. Dickson, *The Internet Immunity Escape Hatch*, 47 BYU L. REV. 1435, 1443 (2022).

[2] 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 [https://perma.cc/LSX2-QLT5].

[3] *See* Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250, 254 (4th Cir. 2009) ("Section 230 immunity, like other forms of immunity, is generally accorded effect at the first logical point in the litigation process.").

[4] *See infra* Part 0.

quickly spread to every corner of the internet but were practically absent from public use when the statute was drafted.

In recent years, United States circuit courts have afforded section 230 immunity in multiple claims involving algorithmic recommendations.[5] While courts have established some workable frameworks, significant questions remain as to the scope of these rulings, causing several judges to write opinions calling for a more thorough examination.[6] Ultimately, judicial language has failed to stay in line with technological advancement, providing only blunt tools for lower courts to shape the appropriate doctrinal contours. As a result, section 230 affords immunity to tech companies in instances that likely fall outside of the statute's original intent.

Given the ubiquity of recommendation algorithms, it is important to understand how section 230 can, or should, apply to these modern tools. The United States Supreme Court petitioner in *Gonzalez v. Google LLC*[7] sought to clear latent ambiguities in section 230 brought to light by recommendation algorithms. Gonzalez sued Google under the Anti-Terrorism Act ("ATA"), claiming that Google aided and abetted terrorism by algorithmically connecting terrorists with content depicting and supporting terrorist acts and ideologies on YouTube (a Google subsidiary).[8] While the Supreme Court was poised to decide whether section 230 immunity was properly granted to Google by the lower courts, a procedural decision in a parallel case determined *Gonzalez*'s outcome, leaving the primary issue open.

Still, the *Gonzalez* litigation is insightful for the differing theories advanced by the petitioner and by the United States government in its amicus brief. Specifically, Gonzalez focused primarily on refuting prong two of the section 230 immunity test, while the government argued that prong three was the better vehicle to negate immunity. While each attack on Google's immunity would have led to the same outcome in *Gonzalez*, this Comment will demonstrate that the strategies would have distinct and impactful follow-on effects upon being adopted by courts. Previous cases—including *Gonzalez*—suggest that litigants and judges favor the prong two theory. However, that strategy is less harmonious with section 230's purpose compared with the prong three strategy is, so it is unlikely to succeed in the long run.

[5] *See infra* section III.0.

[6] *See infra* sections III.0–III.0.

[7] 598 U.S. 617, 620–21 (2023).

[8] *See infra* section III.0.

Not only do the different immunity-breaking strategies have distinct impacts on future court cases, but they also have different implications for consumer technologies and the companies that develop them. If the prong two strategy succeeds at scale, it could open internet companies to litigation in a wider set of cases, increasing their legal risk and cost. On the other hand, the prong three strategy would have a narrower remit. This Comment will explore these differences in depth.

Furthermore, there is a lack of meaningful precedent and legal research closely examining recommendation algorithms from a technical lens. Not all recommendation algorithms are created equal. Different methodologies and underlying goals of recommendation algorithms beget nuanced manifestations of the technology, which could impact the evaluation and outcome of a section 230 immunity claim. Additionally, some internet companies employ recommendation algorithms simply to organize content they themselves create. In part, this Comment seeks to fill the gap in this discourse by applying a technical lens, which is necessary to understand how section 230 can be thoughtfully applied to the wide array of recommendation algorithms.

From a broader perspective, this Comment illuminates the complexities of section 230 immunity for algorithmic recommendations and argues that immunity may not always apply under the current doctrine. Additionally, this Comment dives deep into *Gonzalez* to understand its legal implications for tech companies. To accomplish this, Part I provides background on section 230 and where the doctrine stands today. Part II explores the different types of recommendation algorithms in consumer technologies to illuminate nuances that could impact a section 230 analysis. Part III examines the previous section 230 case law that involves recommendation algorithms to extract key language and concepts undergirding cases that involve recommendation algorithms. Part IV then discusses the broad implications of *Gonzalez* and shows that more analysis is necessary in this area despite the case's resolution. Part V concludes.

I. SECTION 230 OF THE COMMUNICATIONS ACT

Congress passed the Communications Decency Act ("CDA") in 1996 as an amendment to the Communications Act of 1934.[9] The CDA added section 230 to the Communications Act to reduce children's exposure to inappropriate content on the internet while shielding well-meaning actors

[9] VALERIE C. BRANNON & ERIC N. HOLMES, CONG. RSCH. SERV., SECTION 230: AN OVERVIEW 1 (2021).

from liability for providing means and tools for content moderation.[10] Although section 230 interpretations have evolved, studying its origins helps illuminate the trajectory and rationale of the doctrine's development. Section I.A first explores section 230's origins, then section I.B discusses the text, and how the statute functions in courts.

A. Origins of Section 230

In 1994, Prodigy Services Company ("Prodigy") owned and operated a website that enabled its two million users to communicate via digital "bulletin boards."[11] One such bulletin board, Money Talk, was the leading internet forum in the United States for sharing financial information about stocks and investments.[12] Prodigy was hardly the first internet platform that offered digital message boards,[13] but it differentiated itself from competitors by acting as a newspaper of sorts.[14] That is, Prodigy publicly claimed to exercise editorial control over its bulletin boards' content to reflect American family values.[15] Given Prodigy's rapid growth, its scale made manually reviewing messages impractical.[16] As a result, it implemented automated tools to pre-screen posts and contracted with third-party "Board Leaders" who participated in board discussions, moderated content based on Prodigy's policies, and promoted the boards' use.[17]

While Prodigy's content moderation contributed to its success, it also left it vulnerable to liability, which came to a head in *Stratton Oakmont, Inc. v. Prodigy Servs. Co*.[18] Stratton Oakmont was the underwriting firm for Solomon-Page's initial public offering ("IPO") in 1995.[19] Its claim against Prodigy stemmed from a series of anonymous posts on Money

[10] *Id.*

[11] Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 WL 323710, at *1 (N.Y. Sup. Ct. May 24, 1995).

[12] *Id.*

[13] The Electronic Information Exchange System ("EIES") had bulletin board functionality as early as the 1970s. *See e.g.,* MURRAY TUROFF ET. AL, N. J. INST. OF TECH., HOW TO USE ELECTRONIC INFORMATION EXCHANGE SYSTEM (1977) (discussing the functionality of EIES, including bulletin boards).

[14] *Stratton Oakmont*, 1995 WL 323710, at *2.

[15] *Id.*

[16] *Id.* at *3.

[17] *Id.* at *1–2.

[18] *Id.* at *4.

[19] Susan Antilla, *Market Place; Looking Beyond the Flash in the Meteoric Rise of Solomon-Page*, N.Y. TIMES (May 26, 1995), https://www.nytimes.com/1995/05/26/business/market-place-looking-beyond-the-flash-in-the-meteoric-rise-of-solomon-page.html (last visited Apr. 3, 2024).

Talk admonishing Stratton Oakmont and its president for alleged criminal fraud during the Solomon-Page IPO.[20] Stratton Oakmont subsequently sued Prodigy for libel, framing it as the publisher of the purportedly false posts.[21] In its defense, Prodigy claimed it was akin to an "electronic library" and thus not responsible for the allegedly libelous posts, like CompuServe in *Cubby, Inc. v. CompuServe, Inc.*[22] Still, the New York trial court agreed with Stratton Oakmont that Prodigy acted as the posts' publisher.[23] The decision focused on Prodigy's self-proclaimed editorial control over the site's content—a function that CompuServe did not purport to have.[24] Ultimately, the court found Prodigy liable, despite the content originating from, and being moderated by, third parties.

Stratton Oakmont elicited immediate concern from legislators.[25] Representatives Chris Cox and Ron Wyden introduced an amendment to House Bill 1555 in the 1995 legislative session entitled "Online Family Empowerment" just months after the *Stratton Oakmont* decision.[26] In advocating for the amendment, the representatives expressed cautious optimism for the burgeoning internet ecosystem.[27] They acknowledged the internet's immense and growing utility, but were concerned by its potential to expose children to pornographic or otherwise inappropriate content.[28]

Although Senator James Exon's original CDA draft aimed to quell the same concern, Cox and Wyden disfavored Exon's approach because it tasked the Federal Communications Commission with internet censorship.[29] Accordingly, the representatives' amendment aimed to empower parents to moderate their children's internet experiences instead

[20] *Stratton Oakmont*, 1995 WL 323710, at *1.

[21] *Id.*

[22] *Id.* at *4 (quoting Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 137 (S.D.N.Y. 1991)). CompuServe hosted an online "electronic library" that enabled users to access thousands of third-party information sources. *CompuServe*, 776 F. Supp. at 137. CompuServe was sued for libel when one of the third parties, unbeknownst to CompuServe, provided allegedly false information on the electronic library. *Id.* at 138. CompuServe was not found liable because it was merely "a news distributor," not a publisher, and it "may not be held liable if it neither knew nor had reason to know of the allegedly defamatory" statements. *Id.* at 141.

[23] *Id.* at *5.

[24] *Id.*

[25] *See* BRANNON & HOLMES, *supra* note 9, at 5.

[26] *See* 141 CONG. REC. H8468 (1995).

[27] *See* 141 CONG. REC. H8469 (1995) (statement of Rep. Christopher Cox); *see also* 141 CONG. REC. H8470 (1995) (statement of Rep. Ron Wyden).

[28] *See* 141 CONG. REC. H8469 (1995) (statement of Rep. Christopher Cox); *see also* 141 CONG. REC. H8470 (1995) (statement of Rep. Ron Wyden).

[29] *See* Force v. Facebook, Inc., 934 F.3d 53, 78 (2d Cir. 2019).

of the federal government.[30] To that end, the amendment sought to "protect computer Good Samaritans . . . who take[] steps to screen indecency and offensive material for their customers," citing *Stratton Oakmont* as an outcome adverse to the representatives' vision for the internet's future.[31] In 1996, the Cox-Wyden amendment passed and became section 230 of the Communications Act.[32]

B. Section 230: Text and Function

Representatives Cox and Wyden's intent to increase parental control while promoting internet progression is now enshrined in section 230. To leave no doubt as to the statute's primary purpose, the authors titled it "Protection for private blocking and screening of offensive material."[33] In pursuit of that purpose, section 230(b) lays out the statute's policy aims, which include:

> preserv[ing] the vibrant and competitive free market . . . unfettered by Federal or State regulation . . . encourage[ing] the development of technologies which maximize user control . . . [and] remov[ing] disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.[34]

To accomplish these policy goals, the statute established two operative clauses. The first, section 230(c)(1), protects "interactive computer service" providers and users from being treated as the "publisher or speaker of any information provided by another information content provider."[35] The second, section 230(c)(2), immunizes interactive computer service providers and users from liability for: (A) voluntary, good-faith action to "restrict access or availability" of material they deem objectionable and (B) action taken to "enable or make available . . . the technical means to restrict access to" such material.[36]

[30] *See* 141 CONG. REC. H8470 (1995) (statement of Rep. Christopher Cox) ("The message today should be from this Congress we embrace this new technology, we welcome the opportunity for education and political discourse that it offers for all of us. We want to help it along this time by saying Government is going to get out of the way and let parents and individuals control it rather than Government doing that job for us.").

[31] *Id.*

[32] *See* BRANNON & HOLMES, *supra* note 9, at 5.

[33] 47 U.S.C. § 230.

[34] *Id.* § 230(b)(2)–(4).

[35] *Id.* § 230(c)(1).

[36] *Id.* § 230(c)(2)(A)–(B).

Section 230 also includes definitions for some of its key terms.[37] Two terms are particularly prominent in defining section 230's scope. First, "interactive computer service" is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server."[38] Second, an "information content provider" is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[39] Notably, the terms "creation" and "development" are not given specific definitions within the statute.

Section 230 takes several cues from defamation law, likely due to the statute's origins, so understanding defamation's basic functions provides insight into section 230 analyses. Although defamation is a tort, and thus governed by state law, there are core elements that comprise most defamation claims.[40] Broadly, defamation occurs when there is a false and defamatory statement of fact concerning the plaintiff that the defendant published to a third party, which causes actual injury to the plaintiff.[41] One clear way defamation law influenced the construction of section 230 is the word "publisher."[42] In defamation cases, defamatory information is published when it is communicated "intentionally or by a negligent act to one other than the person defamed."[43] While facially simple, the nuances of this definition have become central to modern section 230 jurisprudence.[44]

Although the statute was created in response to defamation concerns, its immunity has been applied broadly to the great benefit of tech companies. In practice, section 230 has become an effective tool for internet companies to avoid arduous litigation and has even been (perhaps

[37] *See id.* § 230(f).

[38] *Id.* § 230(f)(2). "Access software provider" is defined separately in the statute as "a provider of software (including client or server software), or enabling tools that do any one or more of the following: (A) filter, screen, allow, or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content." *Id.* § 230(f)(4).

[39] *Id.* § 230(f)(3).

[40] RODNEY A. SMOLLA, *Elements of the Modern Cause of Action*, 1 LAW OF DEFAMATION § 1:34 (2d ed., Nov. 2022).

[41] *Id.*

[42] *See* 47 U.S.C. § 230(c)(1).

[43] RESTATEMENT (SECOND) OF TORTS § 577 (AM. L. INST. 1977).

[44] *See infra* sections III.0–III.0.

hyperbolically) credited with creating the modern internet.[45] Because section 230 provides a form of immunity, it is applied at the summary judgment stage.[46] Relying on the text of section 230(c), several circuit courts have adopted a three-part test for immunity: (1) the defendant is an interactive computer provider or user (2) whom a plaintiff seeks to treat as a publisher or speaker (3) of information provided by a third-party information content provider.[47] When all three prongs are met, the case is dismissed without additional factfinding, which protects website providers from "having to fight costly and protracted legal battles."[48]

II. RECOMMENDATION ALGORITHMS

Congress passed section 230 in the relatively early days of the publicly available internet.[49] Since then, the internet has evolved both in scale and the underlying technology. When section 230 passed in 1996, website experiences were consistent for all users. For example, when users accessed Amazon.com, the same landing page appeared for everyone, regardless of who they were, where they were, or how they accessed it.[50] However, in 1998, Amazon was among the first internet companies to offer personalized experiences for each registered customer.[51] Jeff Bezos, the founder and then-CEO of Amazon, opined that if "mass customization" tools were implemented wisely, they would "improve people's lives by helping them find things they would never otherwise

[45] *See* Danielle Keats Citron, *How to Fix Section 230*, 103 B.U. L. REV. 713, 717 (2023); JEFFREY KOSSEFF, THE 26 WORDS THAT CREATED THE INTERNET (2019) (discussing section 230's impact on the growth of internet use and internet companies).

[46] *See, e.g.*, Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 591 F.3d 250, 254 (4th Cir. 2009) ("Section 230 immunity, like other forms of immunity, is generally accorded effect at the first logical point in the litigation process.").

[47] *See* F.T.C. v. Accusearch Inc., 570 F.3d 1187, 1196 (10th Cir. 2009); Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100–01 (9th Cir. 2009); Klayman v. Zuckerberg, 753 F.3d 1354, 1357 (D.C. Cir. 2014); *see also* Eric Goldman, *An Overview of the United States' Section 230 Internet Immunity*, *in* OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY 154, 158–59 (Giancarlo Frosio ed., 2020).

[48] *Nemet Chevrolet*, 591 F.3d at 260 (quoting Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1175 (9th Cir. 2008)).

[49] The World Wide Web was created in 1989 by Tim Berners-Lee but the first publicly accessible website did not launch until 1991, preceding the enactment of section 230 by only five years. Josie Fischels, *A Look Back at the Very First Website Ever Launched, 30 Years Later*, NPR (Aug. 6, 2021), https://www.npr.org/2021/08/06/1025554426/a-look-back-at-the-very-first-website-ever-launched-30-years-later [https://perma.cc/9RB3-D2WR].

[50] *See* Leslie Walker, *Amazon Gets Personal with E-Commerce*, WASH. POST, (Nov. 8, 1998), https://www.washingtonpost.com/wp-srv/washtech/daily/nov98/amazon110898.htm (last visited Apr. 13, 2024).

[51] *Id.*

have."[52] Accordingly, he envisioned a future where Amazon would have a personalized store for every user.[53] To realize that vision, Amazon developed and deployed a proprietary recommendation algorithm, which remains foundational to Amazon's site experience.[54] Amazon's focus on recommendations was prescient, as many of the websites and apps in the modern internet ecosystem successfully employ similar techniques.[55]

This section discusses the different types of recommendation algorithms embedded in contemporary consumer technology. First, section II.A gives a technical background on the most common types of recommendation algorithms. Section II.B then explores where the algorithms appear and how the public interacts with them in everyday life.

A. Technical Background on Common Recommendation Algorithms

Recommendation algorithms in consumer technologies are typically built using one of two foundational methodologies: Collaborative Filtering ("CF") or Content-Based Filtering ("CBF").[56] Additionally, with companies striving to provide the most accurate recommendations possible, hybrid approaches have emerged.[57] Given that analyzing section 230 immunity hinges on whether the interactive computer service is being treated as a publisher of the information developed by a third party, it is important to understand how those terms apply to recommendation systems, which requires an examination of the systems' functions. This section will describe each methodology individually.

1. Collaborative Filtering

CF algorithms recommend items to users that similar users have engaged with positively.[58] Based on the entire history of user-item interactions, the algorithm measures similarities between items and

[52] *Id.*

[53] *Id.*

[54] Brent Smith & Greg Linden, *Two Decades of Recommender Systems at Amazon.com*, 21 IEEE INTERNET COMPUTING, no. 3, 2017, at 12.

[55] *Id.* at 13–14 (noting that Netflix and YouTube use algorithms with similar methodology to Amazon's); *see also infra* Part III.0.

[56] *See* Baptiste Rocca & Joseph Rocca, *Introduction to Recommender Systems*, TOWARDS DATA SCIENCE (June 2, 2019), https://towardsdatascience.com/introduction-to-recommender-systems-6c66cf15ada [https://perma.cc/DC59-ZGQD].

[57] *See* Mehrdad Fatourechi, *The Evolving Landscape of Recommendation Systems*, TECHCRUNCH (Sept. 28, 2015), https://techcrunch.com/2015/09/28/the-evolving-landscape-of-recommendation-systems/ [https://perma.cc/ZL7E-3W6H].

[58] *See* FRANCESCO RICCI, ET AL., *Introduction to Recommender Systems Handbook*, *in* RECOMMENDER SYSTEMS HANDBOOK 1, 11 (Francesco Ricci et al. eds., 2011).

users.[59] It then leverages that information to produce new recommendations.[60] The theory behind CF models is that past user-item interactions can sufficiently imply similarities between users or between items, which informs useful predictions based on those estimated similarities.[61] CF Models are subdivided into two main categories: memory-based approaches and model-based approaches.[62]

Memory-based CF approaches rely directly on the user-item interaction ratings matrix for their recommendation predictions.[63] The recommendations can be based either on user similarities or item similarities.[64] User-based systems evaluate the interest a user might have in a particular item based on whether "neighbor" users have expressed interest in that item.[65] Two users are neighbors when they exhibit similar rating patterns.[66] Alternatively, item-based systems evaluate a user's potential interest in a particular item based on that user's expressed interest in neighboring items.[67] Two items are neighbors when they are ranked similarly by many different users.[68] In both methodologies, a user's inputs are directly considered, but optimal recommendations also rely on other users' interactions.

While memory-based CF approaches can produce high-quality recommendations based on relatively simple algorithms, they can be difficult to scale efficiently.[69] As the number of users and items grow, there will be an increasing number of empty cells in the user-item

[59] *See* Rocca & Rocca, *supra* note 56.

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] In simple terms, the data for all CF models (both memory and model-based) is stored in a two-dimensional matrix, which consists of one row for each user, and one column for each item in the system. Where there has been an interaction between a user (x) and an item (y), a value for that interaction is stored in the (x,y) cell of the matrix. When no interaction has occurred, the (x,y) cell will be empty, meaning there is no direct data about how that user interacts with that item. *See* Christian Desrosiers & George Karypis, *A Comprehensive Survey of Neighborhood-based Recommendation Methods*, *in* RECOMMENDER SYSTEMS HANDBOOK 107, 110–111 (Francesco Ricci et al. eds., 2011).

[64] *Id.* at 111.

[65] *Id.*

[66] *Id.* There are many ways to calculate the similarities between users, but the nuances are beyond the scope of this Comment.

[67] *Id.* at 112.

[68] *Id.*

[69] *See* Rocca & Rocca, *supra* note 56 ("One of the biggest flaw [sic] of memory based collaborative filtering is that they do not scale easily: generating a new recommendation can be extremely time consuming for big systems. Indeed, for systems with millions of users and millions of items, the nearest neighbours search step can become intractable if not carefully designed.").

interaction matrix (i.e., creating a "sparse" interaction matrix).[70] Model-based CF approaches can help reduce issues related to sparsity and find latent inferences that memory-based CF algorithms miss.[71]

Model-based CF algorithms go beyond the direct user-item interaction data and capitalize on latent signals in sparse datasets.[72] They accomplish this by abstracting the initial user-item data matrix.[73] Instead of relying solely on direct user-item interactions, model-based CF methods use compact, representative models that help extract insights from sparse user-item interaction data.[74] In other words, these models treat an absence of information as an insight in and of itself.[75] Accordingly, they are able to find similarities between users that have never interacted with the same items, and between items that have not engaged the same users.[76] Although the models are trained on direct user input, the recommendations ultimately come from the abstracted model, not the user-item interactions directly.[77] That is, the model's recommendation is created by the model developer's analysis, not directly from user input.

2. Content-Based Filtering

While CF methods rely solely on past interactions between users and items, CBF methods require additional information about users or items to effectuate recommendations.[78] The additional information required for CBF algorithms can be input by the developer (e.g., categorizing items or determining user attributes through machine learning)[79] or by the users themselves (e.g., user-provided information about themselves, or content they are sharing).[80] CBF algorithms use this information to match users with items that are similar to items in which they have previously expressed interest.[81]

[70] *Id.*

[71] *Id.*

[72] *See* DESROSIERS & KARYPIS, *supra* note 63, at 112.

[73] *Id.* at 140.

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] *Id.* at 112.

[78] *See* Rocca & Rocca, *supra* note 56.

[79] *See* Pasquale Lops et al., *Content-based Recommender Systems: State of the Art and Trends*, *in* RECOMMENDER SYSTEMS HANDBOOK 73, 75 (Francesco Ricci et al. eds., 2011).

[80] *See* Rocca & Rocca, *supra* note 56; *see also* Vatsal Patel, *Recommendation Systems Explained*, TOWARDS DATA SCIENCE (July 12, 2021), https://towardsdatascience.com/recommendation-systems-explained-a42fc60591ed [https://perma.cc/4FAX-RF4Q].

[81] *See* Lops et al., *supra* note 79, at 75.

When a developer uses a CBF algorithm to recommend content to a user, the model derives insights primarily from ratings provided by that user's feedback or behavior.[82] As a result, sparse datasets can hinder the performance of CBF algorithms because they thrive on predicting the type of items a user will interact with based on that user's previous interactions.[83] In contrast, CF algorithms use ratings from other users to fill those gaps, making sparse datasets less of a challenge.[84] In this way, CBF methods rely solely on the inputs of the user seeking recommendations. Still, CBF methods require significant information about users and recommended items, and analyzing that information typically falls to the algorithm's developer.[85]

B. Recommendation Algorithms in Ubiquitous Consumer Technology

While Amazon was among the first companies to successfully employ a recommendation system, it was not the last. Increasingly, our everyday interactions with consumer technology involve some type of recommendation algorithm.[86]

For example, Facebook's News Feed, which is regularly used by more than two billion people globally, employs a highly complex recommendation system.[87] In essence, News Feed is the interface through which Facebook users get content.[88] Facebook users often follow many pages, groups, and people, and those entities' posts comprise the universe of a user's potential News Feed content.[89] The company sees its recommendation system as necessary to maximize utility for its users by showing them only the posts they are most likely to enjoy or interact

[82] *Id.* at 78.

[83] *See* Desrosiers & Karypis, *supra* note 63, at 110–11 ("Recommender systems based purely on content generally suffer from the problems of *limited content analysis* . . . [which] stems from the fact that the system may have only a limited amount of information on its users or the content of its items.") (emphasis in original).

[84] *See* Lops et al., *supra* note 79, at 78; *see also* Desrosiers & Karypis, *supra* note 63, at 111 ("Collaborative approaches overcome some of the limitations of content-based ones. For instance, items for which the content is not available or difficult to obtain can still be recommended to users through the feedback of other users.").

[85] *See* Lops et al., *supra* note 79, at 78.

[86] *See* Fatourechi, *supra* note 57.

[87] *See* Akos Lada, Meihong Wang, & Tak Yan, *How Machine Learning Powers Facebook's News Feed Ranking Algorithm*, ENGINEERING AT META (Jan. 26, 2021), https://engineering.fb.com/2021/01/26/ml-applications/news-feed-ranking/ [https://perma.cc/4NHW-74KQ].

[88] *See id.*

[89] *See id.*

with.[90] To accomplish optimal results, the News Feed algorithm relies heavily on CBF methods by considering the "type of post, embeddings[,] . . . and what the viewer tends to interact with."[91] News Feed is only one example of how Facebook uses recommendation algorithms—it also recommends pages, groups, and new friends.[92] All of these systems incorporate CF methods, which account for similar users' actions and preferences.[93]

Newer platforms are taking algorithmic effectiveness to new heights. TikTok's recommendation algorithm for the For You Page ("FYP") is often lauded as the reason for the company's rapid success.[94] The FYP allows TikTok users to discover new content.[95] The FYP recommendation system, like Facebook's News Feed, contains CBF methods, and analyzes things like user interactions (e.g., likes, shares, follows, comments, and content creation), content information (e.g., captions, sounds, and hashtags), and device settings.[96] However, unlike News Feed, FYP does not require a user to follow a particular account to receive its content.[97] In this regard, FYP departs from previous social media recommendation systems, and "pushes the boundaries of your interests" by serving content to users in which they have not explicitly expressed interest.[98]

[90] *See id.* ("Without machine learning (ML), people's News Feeds could be flooded with content they don't find as relevant or interesting, including overly promotional content or content from acquaintances who post frequently, which can bury the content from the people they're closest to.").

[91] *Id.* Embeddings are algorithmically generated labels that represent features of the content. *See id*.

[92] *See What Are Recommendations on Facebook?*, META, https://www.facebook.com/help/1257205004624246 [https://perma.cc/NLX6-DAEL].

[93] *See How Does Facebook Suggest Groups for Me to Join?*, META, https://www.facebook.com/help/382485908586472 [https://perma.cc/RPR5-2EYY] ("The technology suggests groups based on the information someone has shared on Facebook and what groups people who share things in common with them have joined and participated in."); *see also How Does Facebook Use My Information to Show Suggestions in People You May Know?*, META, https://www.facebook.com/help/1059270337766380 [https://perma.cc/U3E6-X4RB] ("People You May Know suggestions can be . . . people you may have something in common with.").

[94] *See, e.g.*, Alex Hern, *How TikTok's Algorithm Made It a Success: 'It Pushes the Boundaries'*, THE GUARDIAN (Oct. 24, 2022), https://www.theguardian.com/technology/2022/oct/23/tiktok-rise-algorithm-popularity [https://perma.cc/J4AC-293M] ("But the most powerful tool TikTok has to grab users and keep them hooked is the company's feted 'For You Page', the FYP, and the algorithm that populates it.").

[95] *How TikTok Recommends Videos #ForYou*, TIKTOK (June 18, 2020), https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you/ [https://perma.cc/Z89P-9YMY].

[96] *Id.*

[97] *See* Hern, *supra* note 94.

[98] *Id.*

Many companies, like Netflix, employ hybrid systems to overcome deficiencies in individual recommender methodologies.[99] Netflix famously ran a public competition where it provided prize money to engineers who could create the most effective recommender system based on a broad set of user and item data.[100] Based on that information and subsequent research on recommender systems, Netflix determined that there was "no 'silver bullet' [for] the best-performing method" because of the unique nature of its platform and data.[101] As a result, Netflix divides the recommendation problem into sub-tasks, allowing it "to combine a diversity of different approaches."[102] Suffice to say the Netflix recommendation engine is complex, but incorporates traditional methods, including CF and CBF.[103] Unlike social media companies, Netflix content is not user-generated and it increasingly relies on Netflix-produced content, which now comprises over fifty percent of all its U.S. titles.[104]

The most widely used tool that incorporates recommender-like systems is Google.[105] Although Google incorporates characteristics of CBF, it is different than those previously discussed.[106] Unlike content served through Facebook's News Feed or TikTok's FYP, Google's primary function is responding to users' specific queries.[107] Accordingly, the first steps Google takes in response to input is understanding the query.[108] Next, Google ranks potential results based on its understanding of the query and augments the results with its knowledge of the specific user.[109] In this process, the words and meaning of the query are central, where

[99] *See* Fatourechi, *supra* note 57.

[100] *See* JAMES BENNETT & STAN LANNING, KDDCUP '07, THE NETFLIX PRIZE 1, (Aug. 12, 2007).

[101] Harald Steck et al., *Deep Learning for Recommender Systems: A Netflix Case Study*, AI MAGAZINE, 2021, at 7–8.

[102] *Id*.

[103] *Id.* at 7–9.

[104] *See* Kasey Moore, *Netflix Originals Now Make Up 50% of Overall US Library*, WHAT'S ON NETFLIX (Aug. 24, 2022), https://www.whats-on-netflix.com/news/50-of-netflixs-library-is-now-made-of-netflix-originals/ [https://perma.cc/H6JT-TA7J].

[105] Google is the most visited website in the world with nearly ninety billion visits per month, and the website processes approximately 8.5 billion individual searches per day. Maryam Mohsin, *10 Google Search Statistics You Need to Know in 2023*, OBERLO (Jan. 13, 2023), https://www.oberlo.com/blog/google-search-statistics [https://perma.cc/22QY-95TC].

[106] Google uses "[i]nformation such as your location, past [s]earch history, and [s]earch settings" in deciding which results to show. It also personalized results based on "the activity in your Google account." *How Results Are Automatically Generated*, GOOGLE, https://www.google.com/search/howsearchworks/how-search-works/ranking-results/ [https://perma.cc/MUW5-U2UR].

[107] *Id.*

[108] *Id.*

[109] *Id.*

information about the user and content only refine the results. In other words, Google will never show content based simply on users' characteristics or behavior like Facebook and TikTok do—the query is always paramount.

The ubiquity of services embedded with recommendation algorithms has important implications for section 230 litigation. These algorithms change the relationship between platforms and the content they host, which feasibly impacts whether such content is strictly created by third parties as required by prong three of the section 230 immunity test. The following Part gives a brief history of relevant jurisprudence before exploring the cases that have built the budding doctrine specific to recommendation algorithms.

III. RECOMMENDATION ALGORITHMS IN SECTION 230 CASE LAW

When defendant tech companies employ algorithms to recommend content that is central to the plaintiff's allegations, courts have generally found that section 230 immunity offers a shield from liability.[110] However, these cases are relatively new, and not all jurists share consistent opinions on the matter.[111] Given that section 230 was enacted nearly thirty years ago, there is a significant corpus of precedent, which has typically relied on the same three-prong immunity test: (1) that the defendant is an interactive computer service; (2) that the complaint treats the defendant as the publisher; and (3) that the information at issue comes from a third party.[112] Cases involving recommendation algorithms use the same foundation but have adapted to the novel circumstances. Section III.A outlines the relevant foundational section 230 decisions before sections III.B and III.C analyze cases directly involving recommendation algorithms.

A. Information Content Providers and Content Development Under Section 230

Section 230 immunity only applies to defendants when the contested information comes from a different "information content provider."[113] However, the statutory definition of "information content provider" is

[110] *See infra* sections III.0–III.0.

[111] *See id.*

[112] Goldman, *supra* note 47.

[113] *See supra* section I.0.

broad.[114] It encompasses "any person or entity that is responsible, *in whole or in part*, for the *creation or development* of information,"[115] which implies there can be multiple developers.[116] But what constitutes development in this context? Two landmark cases help trace the boundaries of these phrases' legal definitions.

1. Fair Housing Council of San Fernando Valley v. Roommates.com

Fair Housing Council of San Fernando Valley v. Roommates.com[117] was instrumental in defining key terms to section 230's application to recommendation algorithms. Roommates.com ("Roommate") was a website that connected people with spare rooms to potential roommates.[118] Aiming to facilitate fruitful matches, the platform required all users to complete profiles with information about themselves.[119] While some fields prompted users with open text boxes, others required input from a drop-down menu with predefined options provided by Roommate.[120] For example, the site required all subscribers to indicate their sex via a prepopulated drop-down menu.[121] From those drop-down menus, all subscribers seeking roommates had to disclose the sexual orientation of the dwelling's current occupants, and whether children were present.[122] Additionally, the platform forced subscribers seeking housing, via drop-down menus, to specify what sexual orientations they were comfortable with in potential housemates, and whether they would live with children.[123]

The plaintiffs claimed that these questions violated the Fair Housing Act ("FHA"),[124] which prohibits housing discrimination based on "sex" and "familial status," among other classifications.[125] Roommate claimed that section 230 immunity applied because it did not

[114] FTC. v. Accusearch Inc., 570 F.3d 1187, 1197 (10th Cir. 2009) (quoting Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 419 (1st Cir. 2007)) ("This is a broad definition, covering even those who are responsible for the development of content only 'in part.'").

[115] 47 U.S.C. § 230(f)(3) (emphasis added).

[116] *See Accusearch*, 570 F.3d at 1197 ("Accordingly, there may be several information content providers with respect to a single item of information . . . .").

[117] 521 F.3d 1157 (9th Cir. 2008).

[118] *Id.* at 1161.

[119] *See id.*

[120] *Id.* at 1165.

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] 42 U.S.C. § 3604(c).

develop the allegedly violative content by simply providing the questions and drop-down menus—after all, the subscribers "push[] the last button or take[] the last act before publication."[126] The Ninth Circuit Court of Appeals disagreed.[127] Since Roommate provided finite choices for the sensitive categories, it reasoned that "every [profile] page is a collaborative effort between Roommate and the subscriber," making them at least partially responsible for the content's development.[128]

In its opinion, the court grappled with interpreting "develop" in the section 230 context.[129] While the dissent advocated for defining "develop" to overlap with the definition of "create," the majority drew from broader interpretations: "making usable or available" or "the process of researching, writing, gathering, organizing and editing information for publication on web sites."[130]

In applying its definition, the court textually evaluated the statute's information content provider designation.[131] "[R]eading the exception for co-developers as applying only to content that originates entirely with the website . . . ignores the words 'development . . . in part' in the statutory passage 'creation or development in whole or in part.'"[132] While "passive conduits" should surely enjoy section 230 immunity, the opinion argued, co-developers should not.[133] The court further clarified that "providing *neutral* tools" does not amount to development, and should not exempt a defendant from section 230 immunity.[134]

Notably, Roommate's development was only important because it contributed to the content's alleged FHA violation.[135] Since the predefined drop-down menus were central to the complaint's alleged housing discrimination, Roommates "help[ed] to develop unlawful content, and thus f[ell] within the exception to section 230 [immunity]."[136] Critically, *Roommates* held that defendants' actions can only be

[126] *Roommates*, 521 F.3d at 1166.

[127] *Id.*

[128] *Id.* at 1167.

[129] *See id.* at 1167–69.

[130] *Id.* at 1168. The dissent's used the definition "gradual advance or growth through progressive changes." *Id.* at 1184 (McKeown, J., dissenting).

[131] *See Roommates*, 521 F.3d at 1167.

[132] *Id.* (quoting 47 U.S.C. § 230(f)(3)) (emphasis omitted).

[133] *Id.*

[134] *Id.* at 1169 (emphasis in original).

[135] *Id.* at 1167–68.

[136] *Id.* at 1168; *see e.g.*, Vargas v. Facebook, Inc., No. 21-16499, 2023 WL 6784359, at *3 (9th Cir. Oct. 13, 2023), *cert. denied*, No. 23-764, 2024 WL 674871 (U.S. Feb. 20, 2024) (finding that Facebook was a developer of categories used for ad targeting when the categories were generated by a Facebook algorithm).

considered "development" if they contribute to the illegality of the underlying claim.

2. FTC v. Accusearch

In *FTC v. Accusearch*, the Tenth Circuit continued the Ninth Circuit's search for a satisfactory definition of "develop."[137] Accusearch owned and operated a website, Abika.com, that allowed users to access personal information about members of the public.[138] The site acted primarily as an intermediary between users and "third-party researchers," which could find and provide requested personal information, including phone records.[139] Under the Telecommunication Act of 1996, disclosing information related to private phone records is generally prohibited.[140] Accordingly, the FTC claimed that Accusearch's role in commercializing such records violated the Federal Trade Commission Act as an unfair trade practice.[141] Accusearch sought section 230 immunity, claiming that it was being treated as the publisher of the third-party researchers' information.[142]

The Tenth Circuit relied on language from *Roommates* to evaluate whether Accusearch partially developed the content on its website, but the court arguably interpreted "develop" even more broadly.[143] Seeking to differentiate "develop" from "create," as warranted by the statute's language, the court defined "develop" as "the act of drawing something out, making it 'visible,' 'active,' or 'usable.'"[144] Accordingly, Abika.com was found to have developed the phone records when it "exposed [them] to public view."[145]

The court recognized that such a broad reading of "development" could "undermine the purpose of immunity under the CDA."[146] It assuaged this concern by specifying that "a service provider is 'responsible' for the development of offensive content only if it in some way specifically encourages development of what is offensive about the content."[147] Here,

[137] *See* FTC v. Accusearch Inc., 570 F.3d 1187, 1197–98 (10th Cir. 2009).

[138] *See id.* at 1198.

[139] *Id.* at 1191.

[140] 47 U.S.C. § 222(a).

[141] *Accusearch*, 570 F.3d at 1192.

[142] *Id.* at 1193.

[143] *See id.* at 1191.

[144] *Id.* at 1198.

[145] *Id.*

[146] *Id.*

[147] *Id.* at 1199.

the confidential phone records were made “offensive” when they were impermissibly disclosed because such disclosure was the crux of the Telecommunication Act violation.[148] Thus, by knowingly transforming “virtually unknown information into a publicly available commodity,” Accusearch had contributed to the content’s illegality, and was partially responsible for its development.[149]

Roommates was critical to interpreting development in section 230 contexts. It defined development broadly but determined that “neutral tools” receive immunity when they are identically applied in all contexts.[150] *Accusearch* built on this baseline and broadened development to include making information visible, active, or usable. These cases have been instrumental in shaping modern section 230 jurisprudence, including its application to recommendation algorithms.

B. Judicial Interpretations of Whether Algorithms Develop Content

Roommates and *Accusearch* laid the foundation for applying section 230 immunity to algorithmic recommendations by defining development.[151] While courts in the Second, Ninth, and D.C. Circuits have considered section 230 in this context, the concurring opinions and one recent United States Supreme Court case suggest there are critical unanswered questions about the boundaries of section 230 immunity generally, and particularly whether recommendation algorithms develop content. This section discusses the principal cases comprising this nascent doctrine before outlining *Gonzalez v. Google* and its implications.

[148] *Id.*

[149] *Id.*

[150] Although the “neutral tools” test remains foundational to section 230 jurisprudence, a recent unpublished case from the Ninth Circuit, *Vargas v. Facebook, Inc.*, took an arguably narrower view of the doctrine. *See* Vargas v. Facebook, Inc., No. 21-16499, 2023 WL 6784359, at *3 (9th Cir. Oct. 13, 2023), *cert. denied*, No. 23-764, 2024 WL 674871 (U.S. Feb. 20, 2024). The plaintiffs alleged that Facebook violated the FHA by providing tools enabling housing providers to discriminate. *Id.* at *1. The contested tools were like those in *Roommates* because they enabled housing advertisers to “exclude women or persons with children [or] . . . draw a boundary around a geographic location and exclude persons falling within that location.” *Id.* at *2. Facebook sought section 230 protection under the “neutral tools” doctrine from *Roommates*, which the court rejected despite accepting that the contested tools were broadly available, not solely to housing-related advertisers. *Id.* at *3. The court determined that “[a] patently discriminatory tool offered specifically and knowingly to housing advertisers does not become ‘neutral’ within the meaning of this doctrine simply because the tool is also offered to others.” *Id.* Despite the tools being available to all advertisers, which arguably falls within the *Roommates* neutrality framework, the court declined section 230 protection because Facebook’s tools allowed for housing discrimination, even though the tools had other legal uses. *Id.*

[151] *See* BRANNON & HOLMES, *supra* note 9, at 18. (“treatment of algorithmic sorting applies the ‘neutral tools’ language first appearing in *Roommates*.”).

1. Marshall's Locksmith Service Inc. v. Google, LLC

The D.C. Circuit was the first appellate court to apply section 230 to algorithms[152] in June 2019 with *Marshall's Locksmith*.[153] Fourteen locksmith business alleged that Google, Microsoft, and Yahoo! violated false advertising and antitrust statutes by accepting advertising revenue from scam locksmiths that flooded the market with misleading information.[154] Instead of responding to queries with legitimate locksmith listings, the search algorithms served users information about nonexistent physical stores that appeared nearby them due to the scammers' misleading inputs.[155] The complaint alleged that the defendants' failure to remedy the scam harmed the plaintiffs' businesses because location-based internet searches were the "primary means" for finding locksmith services.[156] Among other violations, the plaintiffs claimed that Google's algorithmic "translation" of scammers' false location inputs into map pinpoints categorized Google as an information content provider because it developed the pinpoints.[157]

The appellate court ruled that section 230 immunity applied, affirming the lower court ruling.[158] The false location information originated from the scammers, so Google was not deemed the information content

[152] A Westlaw search of "'Section 230' and algorithm!" returned just sixteen unique results in appellate courts as of March 2024. Although some of the decisions predate *Marshall*, their discussions of algorithms are brief and do not pertain directly to section 230's application to recommendation algorithms. *See* Crosby v. Twitter, Inc., 921 F.3d 617, 620 (6th Cir. 2019) (discussing algorithms in the context of plaintiffs' argument that defendant could have used algorithms to stop the alleged harm); Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1182 (9th Cir. 2008) (mentioning "algorithm" only in the partial concurrent and not related to any section 230 analysis); Google, Inc. v. Hood, 822 F.3d 212, 216–18, 228 (5th Cir. 2016) (discussing a challenge to immunity for Google's search algorithm under section 230, but dismissing the case for lack of ripeness); Rosetta Stone Ltd. v. Google, Inc., 676 F.3d 144, 151 (4th Cir. 2012) (mentioning "algorithm" only once in the context of describing Google's search function); Prometheus Radio Project v. F.C.C., 373 F.3d 372, fn. 103 (3d Cir. 2004), as amended (June 3, 2016) (mentioning "algorithm" only once in a footnote about how news headlines appear on Google Search). One case from the Eleventh Circuit arguably extended section 230 immunity to Google Search's recommendation algorithm, but the specific allegation focused on Google allegedly manipulating its search results as opposed to the functions of the algorithm itself. *See* Dowbenko v. Google Inc., 582 F. App'x 801, 804–05 (11th Cir. 2014).

[153] Marshall's Locksmith Serv. Inc. v. Google, LLC, 925 F.3d 1263 (D.C. Cir. 2019). The algorithms in question were not the search platforms' recommendation algorithms, but the algorithms that converted location data into pin placements on maps. *See id.* at 1270–71.

[154] *Id.* at 1265–66.

[155] *Id.*

[156] *Id.* at 1265.

[157] *See id.* at 1269.

[158] *Id.* at 1272.

provider.[159] Additionally, Google did not partially develop the location information by converting it to pinpoints because it simply provided a "neutral algorithm" that changed the locations' visual representations without altering the underlying information.[160] *Marshall's Locksmith* thus expanded the *neutral tools* framework from *Roommates* to encompass *neutral algorithms* when said algorithms are consistently applied to the content they handle.

2. Force v. Facebook

Approximately two months after *Marshall's Locksmith*, the Second Circuit waded into the discussion with a lengthy analysis specific to Facebook's algorithmic recommendations.[161] The complaint in *Force v. Facebook* alleged that Facebook unlawfully provided Hamas with a communications platform, which enabled deadly attacks on U.S. citizens in Gaza.[162] Under the Anti-Terrorism Act, a party can be liable "for an injury arising from an act of international terrorism committed, planned, or authorized by an organization that had been designated as a foreign terrorist organization" when it "aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism."[163] The plaintiffs sued Facebook under the ATA because the platform's tools and algorithms allegedly enabled Hamas "to disseminate its messages directly to its intended audiences," which they argued was indispensable to actualizing the attacks.[164]

The section 230 analysis partially focused on whether Facebook's recommendation algorithms were responsible for developing Hamas's content.[165] Its analysis drew heavily from *Roommates* and *Marshall's Locksmith*.[166] The court did not find Facebook responsible for the content's development because it did not alter information that its users published, and because the algorithms were "content 'neutral.'"[167] The

[159] *Id.* at 1270.

[160] *Id.* at 1270–71.

[161] *See* Force v. Facebook, Inc., 934 F.3d 53, 68–71 (2d Cir. 2019).

[162] *Id.* at 59.

[163] 18 U.S.C. § 2333(d)(2).

[164] *Force*, 934 F.3d at 59. The specific charges included aiding and abetting the attacks, conspiring with Hamas in the terrorism acts, providing material support to terrorists, and providing material support to a designated foreign terrorist organization. *Id.* at 61.

[165] *Id.* at 68–71.

[166] *See id.*

[167] *See id.* at 70 (quoting Marshall's Locksmith Serv. Inc. v. Google, LLC, 925 F.3d 1263, 1270 (D.C. Cir. 2019)).

majority reasoned that "[m]erely 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."[168] The plaintiffs lobbied for a broader interpretation of "develop[]," akin to the Tenth Circuit's definition in *Accusearch*.[169] However, the court rejected the plaintiffs' characterization, and classified Facebook's actions as nothing more "than Facebook vigorously fulfilling its role as a publisher."[170] Accordingly, punishing platforms for organizing or distributing third-party content was contrary to section 230's purpose in the eyes of the Second Circuit.[171]

Chief Judge Katzmann authored a partial concurrence questioning the majority's treatment of Facebook's algorithms under section 230.[172] Interestingly, Katzmann focuses on whether Facebook should be classified as the publisher of the contested information under section 230(c)(1).[173] However, he also discussed whether Facebook's algorithms develop content through its recommendations.[174] Katzmann asserts that "Facebook uses the algorithms to create and communicate its own message: that it thinks you, the reader—you, specifically—will like this content."[175] This additional message, he argued, pushes Facebook beyond the scope of publishing as defined by section 230.[176] In doing so, he also posited that Facebook's algorithmic recommendations "based on their prior activity on Facebook, including their shared interest in terrorism, 'is directly related to the alleged illegality of the site.'"[177] Katzmann's concurrence was the first judicial acknowledgment that algorithmic recommendations may not be eligible for section 230 immunity because companies use them to communicate their own messages.[178]

[168] *Id.*

[169] *Id.* ("Plaintiffs also argue that Facebook develops Hamas's content because Facebook's algorithms make that content more 'visible,' 'available,' and 'usable.'").

[170] *Id.*

[171] *Id.* at 70–71.

[172] *Id.* at 76 (Katzmann, J., concurring in part).

[173] *Id.* at 80–81.

[174] *Id.* at 82.

[175] *Id.*

[176] *See id.* at 83.

[177] *Id.* at 83.

[178] *See supra* note 150 and accompanying text; *see also* Petition for Writ of Certiorari at i, Gonzalez v. Google LLC, 598 U.S. __, 143 S. Ct. 80 (2022) (No. 21-1333).

3. Dyroff v. Ultimate Software

Just three weeks after *Force*, *Dyroff v. Ultimate Software Grp., Inc.*[179] presented another case involving recommendation algorithms and ushered similar reasoning into the Ninth Circuit.[180] Ultimate Software operated the Experience Project, a website that provided communities and discussion forums for people with similar experiences.[181] One user, Wesley Greer, solicited heroin on a heroin-related group hosted by the Experience Project.[182] After a different user responded to his post, the Experience Project sent Greer an email notifying him of the new information.[183] He connected with the responder, and unknowingly purchased heroin laced with fentanyl.[184] The next day, Greer died from fentanyl toxicity.[185]

Like Katzmann's *Force* concurrence, *Dyroff* considered how recommendation algorithms contribute to classifying defendants as publishers under prong two of section 230.[186] However, the *Dyroff* court departed from Katzmann on how to characterize algorithmic functions: "These functions—recommendations and notifications—are tools meant to facilitate the communication and content of others. They are not content in and of themselves."[187] Since the recommendations and notifications are not information themselves, the court concluded that they are being treated as the publisher of the offending third-party information.

C. Recent Developments in Section 230 Regarding Algorithms: Gonzalez v. Google

In May 2023, the United States Supreme Court decided *Gonzalez v. Google*, another case that alleged ATA violations against internet platforms.[188] The Court initially granted certiorari to clarify how

[179] 934 F.3d 1093 (9th Cir. 2019).

[180] *See id.* at 1098–99.

[181] *Id.* at 1094.

[182] *Id.* at 1095.

[183] The email notification was based on Greer's previous post and was sent algorithmically. However, this algorithm did not recommend the response from whole cloth—it was an automated response to direct input from Greer. *Id.* at 1099.

[184] *Id.* at 1095.

[185] *Id.*

[186] *See id.* at 1097–98.

[187] *Id.* at 1098.

[188] Gonzalez v. Google LLC, 598 U.S. 617, 620–21 (2023).

section 230 applies to algorithmic recommendations.[189] In the Ninth Circuit Court of Appeals, *Gonzalez* was a consolidation of three separate cases: *Gonzalez v. Google*, *Clayborn v. Twitter*, and *Twitter v. Taamneh*.[190] Only two—*Gonzalez*[191] and *Taamneh*[192]—were reviewed by the Supreme Court. Although the Court granted certiorari for each case independently to examine separate issues, *Taamneh*'s disposition ultimately forced *Gonzalez* to resolve without the Court deciding the case's core section 230 issue.[193] Regardless, the *Gonzalez* litigation provided helpful insight into how practitioners are approaching section 230 as applied to algorithmic recommendations, which this section will now explore.

1. Gonzalez *in the Ninth Circuit Court of Appeals*

The facts and allegations in *Gonzalez* are like those in *Force*.[194] ISIS[195] carried out a terrorist attack in Paris in 2015, killing 129 people, including Nohemi Gonzalez, a U.S. citizen.[196] The third amended complaint alleged that Google, through its subsidiary, YouTube, was secondarily liable under the ATA for aiding and abetting terrorism and conspiring with ISIS (the "non-revenue sharing claims").[197] Additionally, the plaintiffs claimed Google was directly liable for providing material support to a known

[189] *See* Petition for Writ of Certiorari at i, Gonzalez v. Google LLC, 598 U.S. __, 143 S. Ct. 80 (2022) (No. 21-1333) ("The question presented is: Does Section 230(c)(1) immunize interactive computer services when they make targeted recommendations of information provided by another information content provider, or only limit the liability of interactive computer services when they engage in traditional editorial functions (such as deciding whether to display or withdraw) with regard to such information?").

[190] Gonzalez v. Google LLC, 2 F.4th 871, 880 (9th Cir. 2021), *vacated and remanded*, 598 U.S. 617 (2023), and *rev'd sub nom.* Twitter, Inc. v. Taamneh, 598 U.S. 471 (2023).

[191] 598 U.S. 617.

[192] 598 U.S. 471.

[193] *Gonzalez*, 598 U.S. at 622 ("[W]e think it sufficient to acknowledge that much (if not all) of plaintiffs' complaint seems to fail under either our decision in *Twitter* or the Ninth Circuit's unchallenged holdings below. We therefore decline to address the application of § 230 to a complaint that appears to state little, if any, plausible claim for relief.") (emphasis in original).

[194] As in *Force*, the underlying allegations stem from the ATA embodied in 18 U.S.C. § 2333. *Gonzalez*, 2 F.4th at 882.

[195] "'ISIS' is shorthand for the Islamic State of Iraq and Syria. In some form or another, it has been designated a Foreign Terrorist Organization since 2004; ISIS has also been known as the Islamic State of Iraq and the Levant, al Qaeda in Iraq, and the al-Zarqawi Network." *Gonzalez*, 598 U.S. at 621, n.1.

[196] Petition for Writ of Certiorari at 10–11, Gonzalez v. Google LLC, 598 U.S. __, 143 S. Ct. 80 (2022) (No. 21-1333).

[197] Gonzalez v. Google LLC, 2 F.4th 871, 882 (9th Cir. 2021), *vacated and remanded*, 598 U.S. 617 (2023), and *rev'd sub nom.* Twitter, Inc. v. Taamneh, 598 U.S. 471 (2023).

terrorist organization by enabling ISIS to monetize videos it uploaded to YouTube (the "revenue sharing claims").[198]

The Ninth Circuit found that section 230 immunity applied to the non-revenue sharing claims.[199] Applying precedent from *Barnes v. Yahoo!*,[200] *Roommates*, and *Force*, the court reasoned that Google was being treated as a publisher in the non-revenue sharing claims because the liability stemmed from allowing ISIS to place content on YouTube.[201] Google was also not considered the content's developer under the same "neutral platform" theory found in *Dyroff* and *Roommates*.[202] While precedential constraints influenced this conclusion, the majority opinion highlighted Katzmann's concurrence in *Force* and the concurrences in *Gonzalez* to question whether YouTube's algorithmic recommendations should be held partially responsible for developing third-party content.[203]

Two judges wrote separately in *Gonzalez*—Berzon, fully concurring, and Gould, concurring in part. Berzon echoed the majority's reasoning that it was bound by precedent to apply section 230 immunity to YouTube for the non-revenue sharing claims. However, he wrote separately to "join the growing chorus of voices calling for a more limited reading of the scope of section 230 immunity."[204] The concurrence goes on to question whether "activities that promote or recommend content or connect users" should be considered publishing under section 230.[205]

Gould's partial concurrence adopted the concerns expressed by Berzon (and by Katzmann in *Force*) but took them further by stating he "would hold that [s]ection 230 of the Communications Decency Act ('CDA') does not bar the Gonzalez Plaintiffs' claims for . . . secondary liability under the ATA."[206] His analysis also hinged on YouTube's characterization as a publisher.[207] Similar to Katzmann's analysis in *Force* regarding Facebook's content and friend suggestions, Gould argued that YouTube's recommendation algorithms "develop[ed] a message to ISIS-

[198] *Id.*

[199] *Id.* at 897.

[200] Barnes sued Yahoo! for negligence when it failed to remove false and sensitive information about her that was added to its platform by a jilted ex-boyfriend, despite her repeated requests. 570 F.3d 1096, 1098–99 (9th Cir. 2009). The court found Yahoo! was being treated as a publisher because the alleged violation stemmed from quintessential publishing function—hosting content and deciding whether it should remain on the site. *Id.* at 1102–03.

[201] *Gonzalez*, 2 F.4th at 892.

[202] *See id.* at 894–95.

[203] *See id.* at 895–97.

[204] *Id.* at 913–14 (Berzon, J., concurring).

[205] *Id.* at 913.

[206] *Id.* at 918 (Gould, J., concurring in part).

[207] *Id.* at 922 ("The factor at issue here is the second.").

interested users"[208] and "deliver[ed] the message that those YouTube users may be interested in contributing to ISIS in a more tangible way."[209]

Furthermore, Gould pushed back on the recent judicial tendency to assume that algorithms are neutral.[210] Instead, he proposed a test for neutrality: "[W]here the website (1) knowingly amplifies a message designed to recruit individuals for a criminal purpose, and (2) the dissemination of that message materially contributes to a centralized cause giving rise to a probability of grave harm, then the tools can no longer be considered 'neutral.'"[211] Furthermore, he asserted that "a lack of reasonable review of content posted that can be expected to be harmful to the public, like ISIS's violent propaganda videos, also destroys neutrality."[212] Gould argued that YouTube's algorithms transcended neutrality by recommending ISIS's violent messages, thus contributing to the content's illegality and undermining Google's status as a mere publisher.[213]

2. Gonzalez *in the United States Supreme Court*

It was not obvious that the Supreme Court would grant certiorari for *Gonzalez* because the case did not present a true circuit split—the circuits that decided section 230 cases regarding algorithmically recommended information uniformly granted immunity to the defendants.[214] Regardless, Gonzalez's petition for certiorari called attention to the growing discourse around section 230 immunity in this context.[215] The initial question presented centered on whether the use of recommendation algorithms can negate an interactive computer service's status as a publisher.[216] However, the petitioner's subsequent brief altered the question presented to

[208] *Id.* at 925.

[209] *Id.* at 924.

[210] *See id.* at 923.

[211] *Id.*

[212] *Id.*

[213] *Id.* at 924.

[214] *See supra* section III.0.

[215] *See* Petition for Writ of Certiorari at i, Gonzalez v. Google LLC, 598 U.S. ___, 143 S. Ct. 80 (2022) (No. 21-1333) ("This is the most recent of three court of appeals' decisions regarding whether section 230(c)(1) immunizes an interactive computer service when it makes targeted recommendations of information provided by such another party. Five courts of appeals judges have concluded that section 230(c)(1) creates such immunity. Three court of appeals judges have rejected such immunity. One appellate judge has concluded only that circuit precedent precludes liability for such recommendations.").

[216] *See id.*

encompass additional arguments.[217] Gonzalez asserted that Google was not being treated as a publisher of information from a *third party* and that Google should not be considered an interactive service provider under section 230.[218]

Gonzalez's primary argument invoked the Berzon, Gould, and Katzmann opinions to question whether Google's recommendation system went beyond traditional publishing functions and, consequently, negated section 230 immunity.[219] The petitioner asserted this position on two levels. First, the brief claimed that the lower courts, and previous cases, have wrongly interpreted "publisher" in section 230(c)(1) to mean the everyday use of that word, as opposed to the legal meaning as derived from defamation law.[220] In the defamation context, the petitioner argued, Google was not being treated as a publisher by Gonzalez because the claim arose from the information being publicized, not from the information itself.[221] Second, even under the plain meaning of "publisher," the brief asserted that Google was not being treated as a publisher because the nature of its platform displaced it from any involvement in creating the contested information.[222]

The brief further argued that YouTube's recommendations included content that YouTube itself created, which would not be protected by section 230 immunity.[223] Primarily, Gonzalez pointed to YouTube-generated URLs and notifications as "information" that should not confer immunity to Google if they contributed to the claim's illegality.[224] Since that information was not generated by a third party, Gonzalez argued that it failed prong three of the immunity test. During oral argument, the petitioner's counsel also mentioned YouTube "thumbnails" as content that was at least jointly created by the video's uploader and YouTube.[225] Because YouTube partially developed the thumbnails, the petitioner argued that any alleged liability derived from the use or distribution of those thumbnails should not be dismissed on section 230 grounds.[226]

[217] *Id.*

[218] *See* Brief for Petitioner at 13–15, Gonzalez v. Google LLC, 598 U.S. __, 143 S. Ct. 80 (2022) (No. 21-1333).

[219] *Id.* at 12–13.

[220] *See id.* at 18–19.

[221] *See id.* at 21–22.

[222] *Id.* at 29–30.

[223] *Id.* at 33–34.

[224] *Id.* at 33–35.

[225] Transcript of Oral Argument at 34, Gonzalez v. Google LLC, 598 U.S. __, 143 S. Ct. 80 (2022) (No. 21-1333).

[226] *Id.* at 33–34.

Although the majority of the petitioner's brief focused on the publisher distinction outlined above, much of the petitioner's oral argument revolved around this line of argumentation.[227]

Gonzalez's brief made an additional argument—that YouTube was not an "interactive computer service" as defined in section 230(f)(2).[228] This challenge hinged on how YouTube, via its recommendations, served content to users that they did not expressly request.[229] Accordingly, the petitioner claimed that YouTube was not providing or enabling "access" to YouTube's servers as required by section 230(f)(2), but rather sending content "at the behest of the server's operator."[230] Thus, the petitioner contended that immunity was not warranted because YouTube was not acting as an interactive computer service as required by prong one of the section 230 inquiry.

In addition to the *Gonzalez* litigants' briefs, seventy-eight parties submitted amicus briefs.[231] Perhaps the most impactful brief was from the United States government in support of vacating the Ninth Circuit judgment granting Google section 230 immunity.[232] The government argued that section 230(c)(1) is most naturally read to afford immunity when the defendant "fail[s] to block or remove third-party content, but not to immunize other aspects of the site's own conduct."[233] The brief described the recommendation process to draw a distinction "between a recommendation and the recommended content."[234] Although the government stopped short of suggesting that the recommendation partially developed the underlying information, it asserted that the recommendation itself was information developed by Google.[235] Because the recommendation was not third-party content, the government reasoned that the Ninth Circuit should not have extended immunity, and

[227] *See id.* at 33–41.

[228] Brief for Petitioner at 43, Gonzalez v. Google LLC, 598 U.S. __, 143 S. Ct. 80 (2022) (No. 21-1333).

[229] *Id.* at 46.

[230] *Id.*

[231] Sabine Neschke, *Summarizing the Amicus Briefs Arguments in Gonzalez v. Google LLC*, BIPARTISAN POL'Y CTR. (Feb. 21, 2023), https://bipartisanpolicy.org/blog/arguments-gonzalez-v-google/ [https://perma.cc/XAX7-5DN2].

[232] Brief for the United States as Amicus Curiae in Support of Vacatur at 35, Gonzalez v. Google LLC, 598 U.S. __, 143 S. Ct. 80 (2022) (No. 21-1333).

[233] *Id.* at 8.

[234] *Id.* at 27.

[235] *Id.*

its ruling must be vacated.[236] The Deputy Solicitor General reinforced this position during oral argument.[237]

While the briefs offered several arguments against section 230 immunity in cases regarding algorithmically recommended content, there are others left on the table. Specifically, the rest of this Comment outlines how prong three of the section 230 immunity test can be effectively deployed when recommendation algorithms are at issue, beyond what the petitioner and the government argued. Drawing from the nature of the technology, and language embedded in the circuit court opinions, such algorithms could be partially responsible for the development of the offending content without relying on abstractions like URLs or notifications, or by considering recommendations as stand-alone information. Examining these arguments provides insights into section 230 litigation strategies, which remain useful because *Gonzalez* did not resolve its primary section 230 question.

IV. SECTION 230 IMMUNITY MAY NOT APPLY WHEN DEFENDANTS USE RECOMMENDATION ALGORITHMS

As noted in Katzmann's *Force* concurrence, platforms convey their own messages when they use recommendation algorithms to serve content without a user's direct prompt.[238] If that message itself contributes to the illegality of the underlying claim, then section 230 immunity will not apply to the defendant.[239] This theory negates the third-party content classification under prong three of the section 230 inquiry, instead of the publisher-focused prong two attack at the heart of *Gonzalez*. While the petitioner's brief in *Gonzalez* also questioned prong three, it focuses on URLs and notifications as the content created by Google, which are not specific to defendants that use recommendation algorithms. However, the U.S. government's amicus brief illuminates another path for challenging prong three—framing algorithmic recommendations as creating an implicit message that can contribute to the underlying content's illegality. The remainder of this Comment will show why focusing on prong three in cases involving recommendation algorithms can be a successful strategy in section IV.A, why litigants should employ it in future cases in section IV.B, and the implications of adopting this strategy at scale in section IV.C.

[236] *Id.* at 28.

[237] *See* Transcript of Oral Argument at 102–05, Gonzalez v. Google LLC, 598 U.S. __, 143 S. Ct. 80 (2022) (No. 21-1333).

[238] Force v. Facebook, Inc., 934 F.3d 53, 76 (2d Cir. 2019) (Katzmann, J., dissenting).

[239] *See* F.T.C. v. Accusearch Inc., 570 F.3d 1187, 1199 (10th Cir. 2009).

A. *Recommendation Algorithms Used by Defendants May Fail Prong Three of the Section 230 Immunity Test*

Defendants must show that they are being sued for information provided by a third party to successfully claim section 230 immunity.[240] Accordingly, if a defendant is sued for information it provided, immunity will not be granted. As previously noted, some judges have acknowledged that recommendation algorithms develop messages on behalf of their creators. The nature of recommendation algorithms also supports this view. Whether the algorithm is built on CF, CBF, or a hybrid model, the algorithm, on behalf of its developer, carries out complicated calculations that create engagement predictions that are far removed from users' inputs. That is, when developers employ recommendation systems, user experiences are heavily dependent on the developer's algorithmic instructions.

The specific model methodology used in an algorithm can illuminate how much a user's input impacts the recommendation. CBF methods, like those found in Facebook's News Feed, thrive on information gathered directly from the user's actions, but also rely on other users' data and information about the content on Facebook. On the other hand, CF methods can benefit from direct user inputs but rely primarily on characteristics of the content and users, which do not necessarily come from direct inputs from the user and may be wholly generated by the company itself. Users and content providers inform the algorithms in both methodologies, but the developer's own analysis ultimately produces the recommendations.

There are two ways to frame the information created by recommendation algorithms: (1) as standalone information (like the government's argument in *Gonzalez*) or (2) as augmentative to the recommended third-party information. In the latter scenario, the algorithm—and its developer, by extension—would be considered a partial developer of the underlying information. To illustrate, consider a piece of content posted to Facebook. Based on the post's characteristics and data previously collected from you and your network, Facebook's algorithm generates information about the likelihood that you will enjoy the content. News Feed then uses that likelihood to rank the third-party post, which dictates whether the post ever sees the light of day. Since Facebook fields billions of posts every day, thousands of which are

[240] 47 U.S.C. § 230(c)(1).

relevant to each user, Facebook's recommendation algorithm undoubtedly dictates which posts get views, and which do not.[241]

Interestingly, Katzmann, Gould, and Berzon framed the recommendation algorithm's new message as potentially negating the platform's status as a publisher. To do so, they defined what a "publisher" is for section 230's purposes and claimed that recommendation algorithms go beyond traditional publishing functions. While that argument may hold weight, their language, and the underlying theory, also invite plaintiff attacks on prong three. Claiming that recommendation algorithms create information of their own aligns better with a prong three challenge because it does not require practitioners to labor over what constitutes "publishing" in an ever-evolving internet media ecosystem. Instead, it enables a straightforward application of whether the defendant is considered an information provider.

When the algorithmic message contributes to (or is the source of) the illegality of a claim, section 230 immunity will not apply because the defendant is not being treated as the publisher of *third-party* content. If the recommendation is framed as independent information, the illegality at issue would need to derive from the recommendation. Alternatively, if the recommendation augments third-party information, the illegality at issue must stem from the wide distribution of the original content or some other consequence of the recommendation. In either case, the defendant would be the publisher of the information it created, precluding section 230 immunity on prong three grounds, but leaving prong two intact.

B. Challenging Section 230 Immunity on Prong Three Negates More Claims Than Challenging Prong Two

While the difference between challenging prong two or prong three of section 230 immunity has little impact on the outcome of ATA claims like those in *Gonzalez* and *Force*, it can have significant implications elsewhere. Defamation law, the original context of section 230 as a response to *Stratton Oakmont*,[242] provides a helpful example.

One core element of a defamation claim is that the defendant must have *published* the content.[243] The petitioner's brief in *Gonzalez* claims that the word "publisher" in section 230(c)(1) is meant to embody the legal

[241] *See* Lada et al., *supra* note 87.

[242] *See* BRANNON & HOLMES, *supra* note 9, at 5.

[243] SMOLLA, *supra* note 40.

meaning from defamation law,[244] which the legislative history of section 230 supports.[245] Arguing that algorithmic recommendations go beyond publishing to challenge prong two of the section 230 immunity test also negates an element of prima facie defamation (i.e., publishing). That is, if an interactive service provider is not a publisher for the purposes of section 230 immunity, how can it be a publisher under defamation law? By this logic, a defamation claim fails if the plaintiff successfully negates prong two by denying that the defendant published the information. But the same claim would not necessarily fail if prong three is negated without challenging the defendant's publisher classification.

However, *Force* and *Gonzalez* are based on ATA claims, which do not incorporate a specific publisher requirement.[246] Those plaintiffs could safely assert that the defendants went beyond publishing to attack prong two of section 230 immunity without negating the underlying claim. As a result, attacking prong three can be successfully deployed in a defamation suit against an interactive computer service.

Note that for claims under the ATA and similar statutes, a plaintiff's argument against section 230 immunity must frame the defendant's recommendation as augmenting the underlying third-party content.[247] Since the underlying claim is about aiding and abetting terrorism, the recommendation itself must be associated with terrorist information to hold any weight. That is not necessarily so for defamation. A defamation claim could be successful through either framing of recommendation algorithms outlined in the previous subsection, depending on the exact allegation. Amplifying information or otherwise indicating its importance could itself be defamatory. It is also feasible that defamatory content only reaches an audience because of amplification by the defendant's recommendation algorithm. Ultimately, a prong three strategy can counter section 230 immunity in defamation suits whether a recommendation is considered standalone information or augmenting third-party information.

[244] Brief for Petitioner at 18–19, Gonzalez v. Google LLC, 598 U.S. __, 143 S. Ct. 80 (2022) (No. 21-1333).

[245] *See* 141 CONG. REC. H8469 (1995) (statement of Rep. Christopher Cox); *see also* 141 CONG. REC. H8470 (1995) (statement of Rep. Ron Wyden).

[246] *See* 18 U.S.C. § 2333 (Liability stems for aiding and abetting in terrorist actions or conspiring with known terrorists with no mention of "publishing.").

[247] This would mean the defendant partially developed the underlying content. *See* Force v. Facebook, Inc., 934 F.3d 53, 70–71 (2d Cir. 2019).

C. Widespread Attacks on Prong Three of Section 230 May Have Significant Legal and Technological Impacts

No matter the plaintiff's method for refuting section 230 immunity, a successful attack does not necessarily beget liability.[248] As noted previously, section 230 immunity, like other forms of immunity, is applied at the summary judgment stage. Consequently, when a court denies section 230 immunity, the case is not dismissed immediately but moves forward to trial with no preordained outcome. Determining the exact resulting liability risk is complex and beyond the scope of this Comment.

Regardless, section 230 was meant to shield internet companies from unwarranted litigation, which would likely be costly notwithstanding the trial's outcome.[249] Although the claims may not succeed, even absent section 230 immunity, the mere threat of protracted litigation could chill economic development and innovation.[250] Additionally, the prong three strategy discussed above may enable avenues for defamation claims against internet platforms, which cuts against the initial intent of section 230 as a response to *Stratton Oakmont*. Given that the strategy inherently applies only when the defendant used a recommendation algorithm for content originating from third parties, it will be confined to those circumstances and will not implicate a significant amount of internet functions. For example, companies that rely entirely or primarily on internally developed content (e.g., Netflix) would experience little impact since they would already fail prong three of section 230 immunity in claims concerning their own content. Still, the prong three strategy could empower more cases against internet platforms.

On the other hand, enabling more cases involving recommendation algorithm to survive summary judgment could provide legal and societal benefits. Discovery would illuminate information about opaque recommendation algorithms, providing better knowledge of these crucial systems to legal practitioners and the public.[251] Given the ubiquity and

[248] *See* Brief for Petitioner at 40–41, Gonzalez v. Google LLC, 598 U.S. __, 143 S. Ct. 80 (2022) (No. 21-1333).

[249] *See* Citron, *supra* note 45, at 754–55; Goldman, *supra* note 47, at 159.

[250] *See* Goldman, *supra* note 47, at 163–165.

[251] *See* Susan Benesch, *Nobody Can See into Facebook*, THE ATLANTIC (Oct. 30, 2021), https://www.theatlantic.com/ideas/archive/2021/10/facebook-oversight-data-independent-research/620557/ [https://perma.cc/PHQ8-TJXS] ("The decisions that their employees and their algorithms make about what to amplify and what to suppress end up affecting people's well-being. Yet the companies are essentially black boxes—entities whose inner workings are virtually unknowable to people on the outside. Particularly in the absence of outside oversight, private

societal importance of recommendation algorithms, more transparency about their functions would be positive.[252]

Moreover, concerns about undercutting the primary thrust of section 230 immunity may be unfounded. Recommendation algorithms were absent from the internet in 1996—when section 230 was passed—so a narrow approach to immunity for recommendation systems can still adhere to section 230's initial intent. Ultimately, section 230 is broadly drafted and leaves room for a judicial interpretation that carves recommendation algorithms out of immunity.[253] Congress should update the statute if it intends section 230(c)(1) to immunize algorithmic recommendations because such a broad interpretation is not obvious from—and somewhat conflicts with—the text and legislative history.[254]

While enabling defamation claims against internet platforms may undermine one of section 230's original goals, the overarching aim of the statute would remain intact—to enable platforms to remove or moderate offensive content without risk of liability. Section 230's title is: "Protection for private blocking and screening of offensive material."[255] This sentiment undergirds the policy goals expressed in the statute, and refusing immunity to algorithmic recommendations would do little to threaten immunity for good Samaritan moderation. This goal is primarily served by section 230(c)(2), which confers immunity for platforms that remove "objectionable" content in good faith or fail to remove content despite their best efforts.[256] Simply put, the heart of section 230 will survive regardless of how litigants and courts treat algorithmic recommendations under the statute.

Perhaps the largest looming question for the prong three strategy is its impact on other popular internet technologies, namely search engines. Google has undoubtedly created considerable public utility through the internet—so much so that the word "Google" transcends the company and acts as a stand-in for conducting any internet search.[257] Given the

companies cannot be expected to work in the public interest. It is neither their purpose nor their role. That's why independent researchers at news organizations, universities, and civil-society groups need to be permitted to pursue and gather knowledge on behalf of the public. Compelling that access and protecting it by law is essential to holding internet platforms accountable.").

[252] *Id.*

[253] *See* Dickinson, *supra* note 1, at 1462–1464.

[254] Although Congressional action may be the ideal way to update section 230, it may not be realistic in the short-term given political dynamics. *Id.* at 1458.

[255] 47 U.S.C. § 230.

[256] *Id.* § 230(c)(2).

[257] *See* Virginia Heffernan, *Just Google It: A Short History of a Newfound Verb*, WIRED (Nov. 15, 2017, 7:00 AM), https://www.wired.com/story/just-google-it-a-short-history-of-a-newfound-verb/ [https://perma.cc/67JY-XY35].

importance of search engines, it is no wonder that courts have consistently afforded them section 230 protection when they provide "neutral" tools that respond to user queries.[258]

The prong three strategy could threaten section 230 immunity for search engines if framed broadly. When responding to a query, Google Search aims to provide the most relevant information. Google inherently makes a recommendation in this quest. If its search recommendation can be characterized as standalone information or as supplemental to the underlying information propagated by a Google search, it could be vulnerable to liability and costly litigation stemming from search results.

However, the key distinction remaining between search engine results and algorithmic recommendations—like those from Facebook or TikTok—is the user's role. When utilizing a search engine, users affirmatively seek specific information, which the model builds its recommendations upon. This is not so for feed-based social media. While Facebook's News Feed will only show posts based on people and pages a user is connected to, the specific content it surfaces is not affirmatively sought each time the user logs on. TikTok's recommendations are even further removed from what users affirmatively seek. While the FYP includes content from creators the user follows, it also recommends posts from others based substantially on what *other* users enjoy.

This distinction is critical because it changes the message each algorithm creates. Recommendations from Facebook's News Feed or TikTok's FYP say, "We think *you will like* this information." But Google Search says, "We think this is the information *you are seeking*." The former is less *neutral*—in the parlance of *Force*, *Dyroff*, and *Roommates*—because the affirmative action comes from the platform, not the user. That is, the message from Facebook or TikTok derives primarily from the company's own insights, while a search engine's message comes primarily from the user, a third party. Thus, recommendations based only loosely on information a user seeks should be more vulnerable to losing section 230 immunity than recommendations based on direct user queries.

[258] *See, e.g.*, Marshall's Locksmith Serv. Inc. v. Google, LLC, 925 F.3d 1263, 1270–71 (D.C. Cir. 2019) ("We have previously held that 'a website does not create or develop content when it merely provides a neutral means by which third parties can post information of their own independent choosing online.'"); Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1169 (9th Cir. 2008) ("If an individual uses an ordinary search engine to query for a 'white roommate,' the search engine has not contributed to any alleged unlawfulness . . . ; providing *neutral* tools to carry out what may be unlawful or illicit searches does not amount to 'development' for purposes of the immunity exception.") (emphasis in original).

CONCLUSION

Recommendation algorithms present significant challenges to courts applying section 230 immunity in cases where the algorithm outputs allegedly contribute to the plaintiff's harm. *Gonzalez* could have defined the scope of section 230 immunity for algorithmic recommendations, but was resolved on different grounds, leaving substantial questions unresolved. But its litigation provides clues to how various arguments might fare in the future. Gonzalez's theory attacking YouTube's publisher classification when it served algorithmic recommendations would not extend to future defamation claims because it inherently negates an element of the underlying claim. However, challenging YouTube's immunity by claiming it partially developed the third-party information would not foreclose defamation plaintiffs from using the same framework.

The prong three strategy aligns better with previous judicial language, but the practical impacts of judicial endorsement of that theory are significant. Although any suit surviving a section 230 immunity claim from the defendant would only lead to liability when successfully argued through trial, the mere threat of costly defamation trials would loom large. The outcome would likely threaten current tech company operations and have a chilling effect on innovation. Still, the benefits of increased transparency and paths toward justice for harmed users may outweigh the costs.