PEPPERDINE UNIVERSITY

Pepperdine Law Review

Volume 50 | Issue 4 Article 3

3-15-2023

Lemmon Leads The Way To Algorithm Liability: Navigating The Internet Immunity Labyrinth

Tyler Lisea

Follow this and additional works at: https://digitalcommons.pepperdine.edu/plr

 Part of the Internet Law Commons

Recommended Citation

Tyler Lisea *Lemmon Leads The Way To Algorithm Liability: Navigating The Internet Immunity Labyrinth*, 50 Pepp. L. Rev. 785 (2023)
Available at: https://digitalcommons.pepperdine.edu/plr/vol50/iss4/3

This Comment is brought to you for free and open access by the Caruso School of Law at Pepperdine Digital Commons. It has been accepted for inclusion in Pepperdine Law Review by an authorized editor of Pepperdine Digital Commons. For more information, please contact bailey.berry@pepperdine.edu.

Lemmon Leads the Way to Algorithm Liability: Navigating the Internet Immunity Labyrinth

Abstract

Congress passed Section 230 at the dawn of the internet era to protect innovators from traditional publisher tort liability. At the time, the internet consisted primarily of basic message boards and informational pages. Courts have interpreted Section 230 to provide internet platforms with sweeping immunity from liability for third-party content.

The statute has aged poorly and is now ill-suited for today's internet tools. Modern social media platforms are more than message board intermediaries because they actively shape and select the information pushed to users via engineered, engagement-enhancing algorithms. Engagement algorithms are not merely neutral tools; web developers intentionally design them to dynamically learn and feed content to users. Social media companies amplify inflammatory and negative content because it yields the highest profits, resulting in documented harm to users. This harm includes eating disorder content that severely impacts teen girls' mental health and misinformation that destabilizes democracies.

Lemmon v. Snap *reveals a new approach to internet liability that could overcome Section 230's broad immunity. There, three teenagers tragically perished in a car accident while distracted by Snapchat's "speed filter" feature. Section 230 did not immunize Snap from liability because the negligent design claim treated Snap as a products manufacturer and not as a publisher or speaker. This Comment connects previously explored theories of algorithm*

liability to real precedent by finding a new foothold in Lemmon *and using a syllogism to liken algorithms to other liability-prone products. Courts should extend the* Lemmon *approach and hold social media companies responsible as product manufacturers for the harm their algorithm products cause.*

TABLE OF CONTENTS

I. INTRODUCTION

When Pasiphae gave birth to a boy with the head and tail of a bull, King Minos did not kill the young beast.[1] Rather, following the Oracle of Delphi's instruction, he protected the newborn monster and enlisted the skilled craftsman Daedalus to build a labyrinth to contain him as he grew.[2] Similarly, Congress protected our young internet with early legislation that shielded it from liability.[3] And just as that unnatural newborn grew into the legendary Minotaur that devoured human flesh, our internet has grown in its immunity into an entity with unforeseen destructive power.[4] Our statutory labyrinth needs a redesign, but in the meantime, the theory of products liability may be our Theseus equipped with a ball of string.[5]

Section 230 of the Communications Decency Act (CDA) provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[6] Congress passed Section 230 in 1996 at the dawn of the internet era to protect innovation from traditional publisher tort liability.[7] At the time, the internet consisted primarily of basic message boards and informational pages—a far cry from the advanced modern platforms that we use today, which were entirely uncontemplated in the 1990s.[8]

The statute shielded internet companies from ill-suited publisher liability, but it has aged poorly and become equally ill-suited for today's internet tools.[9] Courts have interpreted Section 230 to provide internet platforms with sweeping immunity from liability arising out of the content they allow third parties

1. Brittany Garcia, *Minotaur*, WORLD HIST. ENCYCLOPEDIA (Sept. 1, 2013), https://www.worldhistory.org/Minotaur/.

2. *Id.*

3. *See* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 57–77 (2019) (describing the origins of Section 230).

4. Agnieszka McPeak, *Platform Immunity Redefined*, 62 WM. & MARY L. REV. 1557, 1557 (2021).

5. *See infra* Part IV.

6. 47 U.S.C. § 230(c)(1) (2018).

7. *See* KOSSEFF, *supra* note 3, at 57–77.

8. *See* KOSSEFF, *supra* note 3, at 3 ("Only forty million people *worldwide* had any Internet access, a tiny sliver of the more than three billion today.").

9. McPeak, *supra* note 4, at 1557 ("[S]ection 230 is a vital law for allowing free expression online, but it is ill-suited for addressing some of the harms that arise in the modern platform-based economy.").

to share on their platforms.[10]

A key transformation between 1996's infant internet and today's internet remains unaccounted for: modern social media platforms are more than message board intermediaries because they actively shape and select the information pushed to users via engineered, engagement-enhancing algorithms.[11] Modern algorithms are not merely neutral tools that allow users to access information; they are intentionally-designed features that dynamically learn and feed content to users according to what will reap the highest engagement.[12] Social media companies amplify inflammatory and negative content because it yields the highest profits, resulting in documented harm to users.[13] This harm ranges from eating disorder content that severely impacts teen girls' mental health to misinformation destabilizing democracy in the United States and internationally.[14]

Lemmon v. Snap, a recent Ninth Circuit ruling, reveals a new approach to internet liability that could overcome Section 230's broad immunity.[15] In *Lemmon*, three teenage boys tragically perished in a car accident.[16] In their final minutes before the crash, the boys used Snapchat's "speed filter" to record the vehicle's rapid velocity.[17] Two of the boys' parents sued Snapchat for negligent design.[18] The district court held that the CDA barred the parents' claim because Snap, Inc. (Snap) is a publisher of third-party information.[19] The Ninth Circuit reversed, noting that the Snapchat app rewarded users for certain achievements on the platform and that many users believed Snapchat would reward them for recording a "snap" with the speed filter while traveling at over 100mph.[20] The CDA did not immunize Snap from liability because

10. McPeak, *supra* note 4, at 1560.

11. Sang Ah Kim, *Social Media Algorithms: Why You See What You See*, 2 GEO. L. TECH. REV. 147, 148–49 (2017).

12. *Id.*

13. *See, e.g.*, Keach Hagey & Jeff Horwitz, *The Facebook Files: Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead.*, WALL ST. J. (Sept. 15, 2021, 9:26 AM), https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215?mod=article_inline (revealing internal Facebook research into known harm caused to users).

14. *Id.*

15. Lemmon v. Snap, Inc., 995 F.3d 1085 (9th Cir. 2021).

16. *Id.* at 1088.

17. *Id.* The speed filter records and displays Snapchat users' "real-life speed." *Id.*

18. *Id.* at 1090.

19. *Id.*

20. *Id.* at 1091–92.

the negligent design claim treated Snap as a products manufacturer and not as a publisher or speaker pursuant to Section 230.[21]

Scholars have reviewed the mismatch between outdated internet immunity and modern internet tools, and some have advocated for applying products liability to social media algorithms, but gaps remain in establishing algorithms as products.[22] This Comment connects the hope of algorithm liability to real precedent.[23] Building on prior work, this Comment finds a new foothold in *Lemmon* and uses a syllogism to liken algorithms to other liability-prone products to illuminate the internet immunity maze.[24] Courts should adopt the *Lemmon* approach and hold social media companies responsible as product manufacturers for the harm their algorithm products cause.[25]

Part II examines how internet platform immunity has developed over time and details the current Section 230 framework.[26] It admits that imposing traditional publisher liability on internet companies is impractical and would have stifled early dot-com innovation.[27] Further, it reviews how courts have interpreted Section 230 to provide broad, sweeping immunity for internet companies and provides an overview of critiques and legislative reform proposals.[28]

Part III takes a closer look at *Lemmon v. Snap* and similar cases in denying CDA immunity to internet companies by regarding them in their capacity as

21. *Id.* at 1092.

22. *See, e.g.*, McPeak, *supra* note 4 (arguing that current internet regulations are outdated); Michael D. Smith & Marshall Van Alstyne, *It's Time to Update Section 230*, HARV. BUS. REV. (Aug. 12, 2021), https://hbr.org/2021/08/its-time-to-update-section-230 (arguing for Section 230 reform to properly reflect the modern internet); Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV., 401, 419 (2017) (advocating for Section 230 reform according to a duty of care standard); Neil Fried, *The Myth of Internet Exceptionalism: Bringing Section 230 into the Real World*, 5 AM. AFFAIRS 179, https://americanaffairsjournal.org/2021/05/the-myth-of-internet-exceptionalism-bringing-section-230-into-the-real-world/ (last visited Jan. 26, 2023) (arguing for an update to Section 230); Allison Zakon, *Optimized for Addiction: Extending Product Liability Concepts to Defectively Designed Social Media Algorithms and Overcoming the Communications Decency Act*, 2020 WIS. L. REV. 1107 (2020) (applying a defective design product liability theory to social media algorithms).

23. *See Lemmon*, 995 F.3d at 1093 (holding immunity did not protect Snapchat from claims that sought to hold it responsible for its own conduct as the manufacturer of a product).

24. *See infra* Part IV.

25. *See infra* Part IV.

26. *See infra* Part II.

27. *See infra* Part II.

28. *See infra* Part II.

product manufacturers and not publishers.[29] It also examines previous failed attempts to skirt CDA immunity with internet design defect claims and addresses the limitations and obstacles that lawmakers and courts must overcome to apply products liability to engagement algorithms.[30] Notably, courts have previously considered algorithms to be "neutral tools" that facilitate content but are not content themselves, thus falling under Section 230's broad umbrella.[31]

Part IV examines the products liability framework applied in *Lemmon* in light of modern engagement algorithms.[32] It provides a roadmap for understanding design defect claims for internet products and reviews the harm caused by engagement algorithms.[33] It then applies a syllogism: If companies can be liable for harm caused by their products, and if engagement algorithms should be considered products because they go beyond "neutral tools," then internet companies should be liable for harm their algorithms cause.[34]

II. PART I: THE COMMUNICATIONS DECENCY ACT'S BROAD IMMUNITY

This section explores Congress's motivation for enacting Section 230 of the Communications Decency Act and reviews the traditional tort law context underlying its statutory language. This section then reviews how courts have interpreted the statute broadly and appraises critiques and reform proposals.

Traditional tort law imposes liability on publishers for what they print, even when they do not author the content.[35] Defamation liability arises when one publishes a false or defamatory statement, and privacy-based torts arise when one unreasonably intrudes upon the seclusion of another, appropriates someone's name or likeness, unreasonably publicizes private information, or unreasonably places another in a false light before the public.[36] Editorial choices that result in harm to others expose traditional publishers to civil liability, which extends to distributors who knowingly disseminate defamatory

29. *See infra* Part III.
30. *See infra* Part III.
31. *See infra* Part III.
32. *See infra* Part IV.
33. *See infra* Part IV.
34. *See infra* Part IV.
35. McPeak, *supra* note 4, at 1565–66.
36. *See* RESTATEMENT (SECOND) OF TORTS §§ 558, 652A (AM. L. INST. 1977) (explaining elements of a defamation claim and stating the general principles of privacy torts).

content.[37]

At the dawn of the internet age in the 1990s, Congress recognized that internet companies provide a substantially different service from traditional publishers.[38] Internet platforms "served primarily as intermediaries, not as traditional editors or . . . newsstands."[39] The burgeoning new "Cyber Age" promised to democratize communication by giving individuals unprecedented access to information and to one another.[40] As the internet began to boom, lawmakers became concerned about the stifling effect broad civil liability would have on the internet's growth as a forum of free expression.[41] Congress protected the infant internet's development with Section 230 by shielding developers from traditional publisher tort liability.[42]

Two cases from the 1990s illustrate the problem that Congress sought to fix by passing Section 230.[43] In *Cubby, Inc. v. CompuServe Inc.* and *Stratton Oakmont, Inc. v. Prodigy Services Co.*, the plaintiffs sued internet platforms for defamatory posts that third parties created on message boards.[44] In *Cubby*, liability did not attach to a message board operator where it neither moderated

37. McPeak, *supra* note 4, at 1565–66 ("Traditional tort law imposes liability on publishers for the content they choose to publish. Thus, poor editorial choices that result in harm to others may give rise to civil liability.").

38. *See* Mark Tushnet, *Internet Exceptionalism: An Overview from General Constitutional Law*, 56 WM. & MARY L. REV. 1637, 1638 (2015) (describing cyberspace as fundamentally different from the real world, both in its location and its primary purpose).

39. McPeak, *supra* note 4, at 1567.

40. *See* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1603–04 (2018) ("The internet ended the speaker's reliance on the publisher by allowing the speaker to reach his or her audience directly.").

41. *See* 47 U.S.C. § 230(b) (2018) (laying out the statute's motivating policies: to promote the development of the internet, to preserve unfettered competition in the internet marketplace, to promote user control over online activity, and to ensure enforcement of criminal law "to deter and punish trafficking in obscenity, stalking, and harassment by means of computer").

42. McPeak, *supra* note 4, at 1567. Congress's original goal with the CDA was to regulate online obscenity by making it illegal to show minors any indecent content. *See* Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 52–53 (1996). Section 230 was included as an amendment during the legislative process because Congress wanted to protect internet speech in reaction to concerns from the *Prodigy* case discussed below. *Id.* About a year later, the Supreme Court struck down most of the anti-indecency provisions of the CDA, but Section 230 survived. *See* Reno v. Am. C.L. Union, 521 U.S. 844 (1997).

43. *See* Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991); Stratton Oakmont, Inc. v. Prodigy Services Co., No. 031063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (unpublished).

44. *Cubby*, 776 F. Supp. at 138; *Prodigy*, 1995 WL 323710, at *1.

content nor attempted to remove improper materials.[45] But in *Prodigy*, a similar computer service was liable because it had attempted and failed to moderate offensive content.[46] There, the defendant internet platform's "conscious choice, to gain the benefits of editorial control, . . . opened it up to a greater liability than . . . other computer networks that make no such choice."[47] Internet services thus faced greater liability if they made an effort to moderate offensive content because an imperfect attempt gave rise to publisher-based defamation claims.[48] *Cubby* and *Prodigy* demonstrated why traditional publisher liability is ill-suited for the internet—trying but failing to do the right thing is punished, while simply doing nothing to moderate is rewarded.[49] This undesirable reality set the stage for Section 230's enactment and subsequent judicial expansion.[50]

45. *Cubby*, 776 F. Supp. at 140–41. A third party uploaded allegedly defamatory content and CompuServe allowed it to be displayed almost instantaneously with no editorial discretion. *Id.* at 140 & n.1. The court held that CompuServe functioned more like a bookseller or library and classified it as a distributor that could only be liable if it knew of the defamatory content, which the plaintiffs had not alleged. *Id.* at 140.

46. *Prodigy*, 1995 WL 323710, at *5. A user of the defendant's forum posted disparaging comments about the plaintiff investment firm. *Id.* at *1. The comments included an allegation that the firm's president "committed criminal and fraudulent acts in connection with the initial public offering of stock" that was "criminal fraud." *Id.* The court held the forum liable as the publisher of defamatory content because it used moderators and software tools to selectively filter out some offensive content but failed to remove the defamatory posts at issue. *Id.* at *4. The court rejected the defendant's argument that it could not perform editorial functions on some sixty-thousand posts per day. *Id.* at *3. Of course, the defamatory statements turned out to be true. *See* Connor Clarke, *How the Wolf of Wall Street Created the Internet*, SLATE (Jan. 7, 2014, 4:29 PM), https://slate.com/news-and-politics/2014/01/the-wolf-of-wall-street-and-the-stratton-oakmont-ruling-that-helped-write-the-rules-for-the-internet.html. You may recognize the name of the allegedly felonious brokerage firm in *Prodigy*; Stratton Oakmont was Jordan Belfort's firm—"The Wolf of Wall Street" himself. *Id.* Stratton Oakmont won this defamation suit, but it would close its doors in disgrace the following year amidst money laundering and securities fraud convictions. *Id.*

47. *Prodigy*, 1995 WL 323710, at *5.

48. McPeak, *supra* note 4, at 1569. As noted in *Prodigy*, the platform's "conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than CompuServe and other computer networks that make no such choice." 1995 WL 323710, at *5. The court held that Prodigy needed to face the legal consequences that flowed from its decision to expand its market and attract more users by becoming a "family-oriented" online forum. *Id.*

49. McPeak, *supra* note 4, at 1569.

50. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008) (en banc) (explaining how *Prodigy* inspired Section 230).

A. Overview of Section 230

Section 230 begins by laying out the congressional findings that inspired broad immunity for internet companies.[51] Subsection (a) notes that the internet represents an "extraordinary advance" for citizens' access to "educational and informational resources" and that users can exercise a great degree of control over the information they receive.[52] The internet offers "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[53] Finally, Congress noted that the internet had thus far flourished with minimal government regulation, and Americans are increasingly relying on it for "political, educational, cultural, and entertainment services."[54]

Subsection (b) lays out key policies underlying the statute, including promoting further internet development and preserving the competitive internet market without state or federal law constraining it.[55] Another policy encourages companies to develop technology that maximizes user control over what information people receive.[56] Some scholars have noted that this policy acknowledges that a free and open internet will inevitably include some undesirable content, and platforms should be free to moderate such content without fearing liability.[57] Other stated policies include removing obstacles for developing parental-control tools to restrict children's access to inappropriate material and ensuring vigorous enforcement of federal criminal laws to "punish trafficking in obscenity, stalking, and harassment."[58]

Section 230's most cited immunity provision is found in subsection (c), entitled "PROTECTION FOR 'GOOD SAMARITAN' BLOCKING AND SCREENING OF OFFENSIVE MATERIAL."[59] Modern broad internet immunity grows from distinguishing between the role of the "provider or user" and the "publisher

51. *See* 47 U.S.C. § 230(a) (2018).
52. *Id.* § 230(a)(1)–(2).
53. *Id.* § 230(a)(3).
54. *Id.* § 230(a)(4)–(5).
55. *Id.* § 230(b)(1)–(2).
56. *Id.* § 230(b)(3).
57. McPeak, *supra* note 4, at 1570–71 ("[A] free and open internet will necessarily include offensive or undesirable content, and platforms should be free to selectively curate content and create user controls without fear of liability.").
58. *See* § 230(b)(4)–(5).
59. *Id.* § 230(c).

or speaker."[60] Specifically, subsection (c) states:

> (1) TREATMENT OF PUBLISHER OR SPEAKER
>
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (2) CIVIL LIABILITY
>
> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[61]

Essentially, immunity turns on a binary classification: whether a company is a computer service or a content provider, and only the "interactive computer service" is afforded immunity.[62]

So, what constitutes an "interactive computer service"? As defined in subsection (f), an interactive computer service enables access to a server.[63] Courts have classified search engines,[64] message board operators,[65] some

60. *Id.*

61. *Id.*

62. McPeak, *supra* note 4, at 1572.

63. § 230(f)(2) (defining "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions").

64. *See, e.g.*, Parker v. Google, Inc., 242 F. App'x 833, 836–38 (3d Cir. 2007) (holding that a search engine which included defamatory content and content that was protected by intellectual property rights was not liable).

65. *See, e.g.*, Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 415 (1st Cir. 2007)

online marketplaces,[66] internet service providers,[67] domain-name registrars,[68] and website hosting services[69] as computer services.[70] The statute defines an "information content provider" as one who is responsible for creating and developing content.[71] "Content providers generally are not immune under section 230."[72] Courts conduct a fact-specific inquiry into the nature of the company's activity to assess whether the company created or developed the problematic content.[73] Traditional tort law sheds light on how the judiciary has crafted and interpreted this language.[74]

Section 230's framework relies on defamation legal concepts.[75] In tort law, a defamation cause of action arises when an actor publishes a false or defamatory statement.[76] "Publication" means communication to someone else, intentionally or negligently, verbally or in print.[77] "A communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or

(holding that a message board which displayed anonymous third-party defamatory content was not liable).

66. *See, e.g.*, Schneider v. Amazon.com, Inc., 31 P.3d 37, 38–39, 43 (Wash. App. Div. 1 2001) (holding that Amazon was not responsible for allowing negative reviews to remain posted despite take-down requests).

67. *See, e.g.*, Noah v. AOL Time Warner Inc., 261 F. Supp. 2d 532, 538 (E.D. Va. 2003) (holding that an internet service provider that provides access to public chatrooms qualified as an interactive computer service), *aff'd*, No. 03-1770, 2004 WL 602711 (4th Cir. 2004).

68. *See, e.g.*, Smith v. Intercosmos Media Grp., Inc., No. Civ.A. 02-1964, 2002 WL 31844907, at *3 (E.D. La. Dec. 17, 2002).

69. *See, e.g.*, Ricci v. Teamsters Union Loc. 456, 781 F.3d 25, 26 (2d Cir. 2015).

70. McPeak, *supra* note 4, at 1572.

71. *See* 47 U.S.C. § 230(f)(3) (2018) (defining "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service").

72. McPeak, *supra* note 4, at 1572.

73. *See, e.g.*, FTC v. LeadClick Media, LLC, 838 F.3d 158, 174 (2d Cir. 2016) (holding that a defendant shall not be treated as an information content provider unless it "assisted in the development of what made the content unlawful"); FTC v. Accusearch Inc., 570 F.3d 1187, 1199 (10th Cir. 2009) (holding that one must act as more than a "neutral conduit" for offensive content to be responsible for it). The court likened a message board to a hypothetical highway used by a fleeing bank robber to illustrate how untenable it would be to hold the highway builder or message board creator responsible for another's conduct. *Id.*

74. McPeak, *supra* note 4, at 1573.

75. *See id.* ("[A] key feature of the statute is its reliance on defamation law concepts in its framework.").

76. *See* RESTATEMENT (SECOND) OF TORTS § 558 (AM. L. INST. 1977) (defining defamation).

77. *See id.* § 577 & cmt. a.

dealing with him."[78] Thus, a defamation claim requires a false and defamatory statement,[79] unprivileged publication of the statement, negligence or greater fault,[80] and sometimes a showing of special harm.[81] Distributors can also be liable if they intentionally fail to remove defamatory content in their control.[82]

Relying on these tort definitions, Section 230 expressly qualifies that a computer service is not to be treated as a "speaker" or "publisher" of third-party content, carving out interactive computer services from defamation liability.[83] Although Congress built Section 230 on this narrow defamation framework, courts have expanded immunity by applying it broadly.[84]

B. Expanding Section 230 Immunity

The year after Congress passed the CDA, plaintiff Ken Zeran brought defamation claims against AOL after an anonymous user posted a fake and offensive t-shirt ad on an AOL message board.[85] The ad included Zeran's phone number, resulting in many angry and threatening phone calls.[86] AOL told Zeran that the ad would be taken down but that company policy prevented them from publishing any retraction.[87] More fake ads kept appearing, and Zeran repeatedly asked AOL to stop them.[88] Zeran sued for negligence based on AOL's alleged unreasonable delay in removing the defamatory messages,

78. *See id.* § 559.

79. *See id.* § 581A & cmt. a. True statements do not give rise to defamation liability. *Id.*

80. *See id.* § 580B. A plaintiff must only prove negligence for private matters regarding private persons, but reckless or intentional behavior is required for cases regarding public figures. *See id.* § 580A.

81. *See id.* § 558 (listing defamation elements); *see also, e.g.*, *id.* §§ 569–70, 575, 620–22 (containing the various special harm provisions).

82. *See id.* § 577(2) ("One who intentionally and unreasonably fails to remove defamatory matter that he knows to be exhibited on land or chattels in his possession or under his control is subject to liability for its continued publication.").

83. 47 U.S.C. § 230(c)(1) (2018); *see* McPeak, *supra* note 4, at 1574.

84. *See infra* Part II.B.

85. Zeran v. Am. Online, Inc., 129 F.3d 327, 329 (4th Cir. 1997). The fake t-shirts in the ad displayed tasteless jokes about the recent Oklahoma City bombing. *Id.* These slogans included "Visit Oklahoma . . . It's a BLAST!!!" and "Finally a day care center that keeps the kids quiet—Oklahoma 1995." Zeran v. Am. Online, Inc., 958 F. Supp. 1124, 1127 nn.3, 5 (E.D. Va.), *aff'd*, 129 F.3d 327 (4th Cir. 1997).

86. *Zeran*, 958 F. Supp. at 1127. Zeran received a call about every two minutes. *Id.* At one point, an Oklahoma City radio station urged its listeners to call Zeran to complain. *Id.*

87. *Id.*

88. *Id.*

failure to post retractions, and failure to prevent future, similar messages from being posted.[89] Zeran argued that AOL should at least be liable as a distributor of defamatory content, thereby responsible for taking down the posts once on notice.[90]

The trial court held that Section 230 barred Zeran's claims, and the Fourth Circuit affirmed.[91] First, AOL is an interactive computer service because it allows users to access the internet, and it stores a network of information created by its users.[92] Second, the court examined the plain language of Section 230, and concluded that it created immunity from any claim which seeks to hold a computer service liable for third-party content.[93] Third, the court cited the goals of promoting discourse and facilitating industry growth with minimal interference and noted that Section 230 encourages computer services to self-regulate without fear of liability.[94] While online harassment is a concern, the court reasoned that Congress had made a policy choice not to deter harmful online speech by imposing tort liability on intermediaries for third parties' potentially injurious messages.[95] This early, broad interpretation of Section 230 immunity shaped decades of internet jurisprudence.[96]

C. Cases Applying Section 230 Immunity to Internet Claims

Section 230 immunity has consistently prevailed in cases regarding internet products and services.[97] In *Herrick v. Grindr LLC*, a dating application, Grindr, was held to be immune under Section 230 when a victim of severe

89. *Zeran*, 129 F.3d at 328. *See generally* Eric Goldman, *Who Cyber-Attacked Ken Zeran, and Why?*, *in* LEGAL STUDIES RESEARCH PAPER SERIES NO. 2017–18 (Santa Clara Univ. Sch. of L. 2017) (speculating on who may have been the culprit attacking Zeran online).

90. *Zeran*, 129 F.3d at 330, 332. Zeran never directly sued the party responsible for posting the ads because he could not determine their identity. *Id.* at 329 & n.1.

91. *Id.* at 328.

92. *Id.* at 329.

93. *Id.* at 330. Accordingly, the court did note that the anonymous third party who created the content was not immune from tort liability. *Id.*

94. *Id.* at 330–31.

95. *Id.*

96. *See* Eric Goldman, *The Ten Most Important Section 230 Rulings*, 20 TUL. J. TECH. & INTELL. PROP. 1, 3 (2017) ("Two decades later, *Zeran* remains the seminal Section 230 opinion, and it has been cited in hundreds of other cases.").

97. *See id.* at 2 (describing Section 230 as "the law that gave us the modern Internet," the "most important law in tech," and "the law that makes the Internet go").

harassment facilitated by the application sued.[98] The plaintiff's ex-boyfriend created a fake Grindr account in the plaintiff's name and used it to direct other Grindr users to harass him at his home and workplace.[99] The plaintiff alleged defective product design—specifically, Grindr's geolocation features, inability to block and prevent spoofing, and lack of safety features—as a basis for his claim.[100] Nonetheless, the court regarded the claims as seeking to hold Grindr liable as the "publisher" of third-party content and the conduct as essentially arising out of third-party use of the application, not the platform's.[101]

In *Doe v. Backpage.com, LLC*, three underage girls became victims of sex trafficking when they were sold on the defendant's website.[102] Plaintiffs alleged that Backpage intentionally enhanced the "escorts" section of its website to maximize profits by making sex trafficking more accessible in the wake of Backpage's competitor, Craigslist, closing its "adult services" section.[103] Plaintiffs alleged that Backpage intentionally structured its website to facilitate sex trafficking by tailoring its posting requirements and advertisement rules.[104] Specifically, Backpage removed postings that were involved in law enforcement sting operations and metadata from escort photos to limit their usefulness to law enforcement.[105] Backpage only charged a posting fee for its "adult" section and charged an extra fee for users to post "sponsored ads" that appeared on every page in the "escorts" section and included a picture of the advertised individual with her location and availability.[106]

Plaintiffs asserted a civil conspiracy claim against Backpage under the Trafficking Victims Protection Reauthorization Act of 2017,[107] which includes a private right of action against anyone who knowingly benefits from participating in a venture which that person knew or should have known was involved with sex trafficking.[108] The First Circuit held that Backpage was

98. Herrick v. Grindr LLC, 765 F. App'x 586 (2d Cir.), *cert. denied*, 140 S. Ct. 221 (2019).
99. *Id.* at 588.
100. *Id.* at 590.
101. *Id.* at 590–91.
102. Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 16–17 (1st Cir. 2016).
103. *See id.* at 16.
104. *See id.* at 16–17.
105. *See id.* at 16.
106. *See id.* at 17.
107. 22 U.S.C. §§ 7101–14 (2017).
108. *See Backpage.com*, 817 F.3d at 15, 17 ("The first set consists of claims that Backpage engaged in sex trafficking of minors as defined by the TVPRA and its Massachusetts counterpart."); 18 U.S.C. § 1595(a) (2018).

immune from civil liability because all claims related to sex trafficker escort listings on Backpage involved information provided by someone else.[109] "Whatever Backpage's motivations, those motivations do not alter the fact that the complaint premises liability on the decisions that Backpage is making as a publisher with respect to third-party content."[110] In direct response to the *Backpage* decision, Congress enacted the Allow States and Victims to Fight Online Sex Trafficking Act of 2017, which amended Section 230 to permit certain sex trafficking claims against online entities.[111]

Dyroff v. Ultimate Software Group Inc. also illustrates Section 230's expansive immunity and will be further explored in Part IV because of its relevance to the argument regarding algorithms.[112] To summarize, an internet platform's recommending algorithm connected a drug dealer to the decedent in a heroin-related forum.[113] The defendant designed the website to allow anonymous use, and the platform's algorithm connected the drug dealer and the decedent by creating topical discussion groups.[114] The court ruled that Section 230 shielded the platform from liability because providing recommendations to users is an ordinary, neutral function of social networking websites.[115] According to the court, the platform functioned merely as an intermediary that used neutral tools to provide a framework that could be utilized by third parties for proper or improper purposes, and it did not create or develop the information even in part.[116]

Daniel v. Armslist, LLC and *Stokinger v. Armslist, LLC* both involved design features of the defendant's website, which allowed an individual to illegally acquire a gun that he used to murder and injure others.[117] Section 230 again applied in both cases because the claims sought to treat the interactive computer service provider as the publisher of information posted by a third

109. *Backpage.com*, 817 F.3d at 21.
110. *Id.*
111. H.R. 1865, 115th Cong. (2d Sess. 2018) (codified as amended in scattered sections of 18 & 47 U.S.C.).
112. Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093 (9th Cir. 2019); *see infra* Part IV.
113. *Dyroff*, 934 F.3d at 1095.
114. *Id.*
115. *Id.* at 1097.
116. *Id.*
117. Daniel v. Armslist, LLC, 386 Wis. 2d 449 (2019), *cert. denied*, 140 S. Ct. 562 (2019); Stokinger v. Armslist, LLC, No. 1884CV03236F, 2020 WL 2617168 (Mass. Super. Ct. April 28, 2020) (unpublished).

party.[118]

Suffice to say, Section 230's immunity has blocked many fierce challengers.[119] The caselaw has established sweeping immunity, creating a legal landscape inequitably slanted to give internet companies the high ground and allowing them to escape liability.[120] But note one crucial distinction: the plaintiffs in these prior cases often tried to establish liability according to how an internet product facilitated a third-party wrongdoer, whereas this Comment follows *Lemmon*'s lead and argues for liability according to harm from the internet product itself.[121] This application is necessary to fill a gap in the interim, but our statutory regulations also need a redesign to appropriately address the modern internet's impact.[122]

D. Revising Section 230

Section 230 has been hotly debated in the quarter-century since its enactment.[123] Much of the currently-contested questions arise from technology's modern capabilities that Congress did not contemplate when enacting the statute.[124] Lawmakers and legal scholars have suggested a variety of proposals, mostly adopting a "carrot-and-stick approach, by tying a platform's safe-harbor protections to its use of reasonable content-moderation policies."[125] A representative example of such a reform proposal would revise Section 230 with the following emphasized changes:

> No provider or user of an interactive computer service that *takes reasonable steps to prevent or address unlawful uses of its services* shall be treated as the publisher or speaker of any information provided by another information content provider *in any action arising out of the publication of content provided by that information content*

118. *Daniel*, 386 Wis. 2d at 457; *Stokinger*, 2020 WL 2617168, at *4.
119. *See generally* Goldman, *supra* note 99 (reviewing ten of the most important victories for Section 230 immunity).
120. *See generally id.* (reviewing cases that allocated internet service providers with expansive Section 230 immunity)
121. *See infra* Part IV.
122. *See* Smith & Van Alstyne, *supra* note 22 (arguing for revision to the outdated Section 230).
123. *Id.*
124. *Id.*
125. *Id.*

provider.[126]

This approach is rooted in the common law "duty of care" standard.[127] The duty of care imposes an obligation for businesses to take reasonable steps to not cause harm to their customers as well as to take reasonable steps to prevent harm to their customers.[128] This standard also creates an affirmative obligation to prevent people from using the business's services to harm others.[129] Thus, by revising the duty of care, internet platforms could be liable if they create an unsafe environment as well as if they fail to prevent one user from using the platform to harm another user.[130] This revision could be an effective check against the decades of sweeping immunity internet companies have enjoyed and help ensure that the internet platforms we use are safe.[131]

On the other hand, defenders of Section 230 argue that the statute as currently written continues to enable innovation, especially because startups and other small businesses may not have sufficient resources to protect their internet sites and tools with the same level of care as large companies.[132] They credit Section 230 for creating the modern internet and maintain that it is still necessary to foster free speech and innovation, and they advocate that repeal or reform would have a stifling effect.[133] According to these scholars, imposing a reasonable care requirement would burden internet companies and

126. Citron & Wittes, *supra* note 22, at 419. Mark Zuckerberg himself echoed the reasoning from this argument in testimony he gave to Congress in 2021. *Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation: J. Hearing Before the Subcomms. On Consumer Prot. & Com. & Commc'ns & Tech. of the H. Comm. On Energy and Com.*, 117th Cong. (2021) (statement of Mark Zuckerberg, Chairman & Chief Exec. Office, Facebook, Inc.).

127. *See* Smith & Van Alstyne, *supra* note 22 ("The duty-of-care standard is a good one, and the courts are moving toward it by holding social media platforms responsible for how their sites are designed and implemented. Following any reasonable duty-of-care standard, Facebook should have known it needed to take stronger steps against user-generated content advocating the violent overthrow of the government. Likewise, Pornhub should have known that sexually explicit videos tagged as '14yo' had no place on its site.").

128. Fried, *supra* note 22.

129. *Id.*

130. *Id.*

131. Citron & Wittes, *supra* note 22, at 419.

132. Smith & Van Alstyne, *supra* note 22.

133. *See* KOSSEFF, *supra* note 3, at 3 ("In the two decades since Section 230's passage, those twenty-six words have fundamentally changed American life. . . . 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, but by users.").

threaten public access to the tools we rely on.[134] However, these arguments seem to neglect that proposed change to the duty of care would impose moderation on content that the First Amendment does not insulate in the first place, thereby protecting users without holding platforms to an unrealistic standard.[135] These criticisms concentrate on third-party content moderation and fail to address the part of the duty of care that, like *Lemmon*, focuses on the company's own conduct.[136]

Although current President Joe Biden and several members of Congress from both sides of the aisle have stated that Section 230 must be repealed or reformed, the original wording of the statute remains in effect.[137] Currently, the California state legislature is considering a bill that aims to hold social media companies liable for addicting children to their platforms.[138] This is a step in the right direction in the immunity labyrinth, but legislative reform may be too slow to compete with the internet Minotaur's break-neck pace,

134. *See* Will Duffield, *Circumventing Section 230: Product Liability Lawsuits Threaten Internet Speech*, CATO INST. (Jan. 26, 2021), https://www.cato.org/policy-analysis/circumventing-section-230-product-liability-lawsuits-threaten-internet-speech (arguing the *Grindr* and *Armslist* cases attempting to circumvent Section 230 immunity "contravene the statute's purpose and threaten Americans' access to the tools upon which they increasingly rely").

135. *See* Smith & Van Alstyne, *supra* note 22 ("There are no First Amendment protections for speech that induces harm (falsely yelling 'fire' in a crowded theater), encourages illegal activity (advocating for the violent overthrow of the government), or that propagates certain types of obscenity (child sex-abuse material).").

136. *See* Duffield, *supra* note 137 (resisting Section 230 revision proposals because inconsistent understandings of what constitutes reasonable moderation would "create an effective standard more restrictive than the sum of its parts.").

137. Smith & Van Alstyne, *supra* note 22. Biden told the New York Times that Section 230 should be "revoked, immediately." *Joe Biden: Former Vice President of the United States*, N.Y. TIMES (Jan. 17, 2020), https://www.nytimes.com/interactive/2020/01/17/opinion/joe-biden-nytimes-interview.html. Congressmen Christopher Cox (R-CA), a co-author of Section 230, has called for rewriting Section 230 because "[t]he original purpose of this law was to help clean up the Internet, not to facilitate people doing bad things." Alina Selyukh, *Section 230: A Key Legal Shield for Facebook, Google Is About to Change*, NPR: ALL TECH CONSIDERED, https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change (Mar. 21, 2018, 5:17 PM).

138. *See* Katie Deighton, *California Bill Aims to Make Tech Firms Liable for Social-Media Addiction in Children*, WALL ST. J. (Mar. 15, 2022, 6:19 PM), https://www.wsj.com/articles/california-bill-aims-to-make-tech-firms-liable-for-social-media-addiction-in-children-11647382786?page=1 ("The bill would let parents and guardians sue platforms that they believe addicted children in their care through advertising, push notifications and design features that promote compulsive use, particularly the continual consumption of harmful content on issues such as eating disorders and suicide."). The bill, called the Social Media Platform Duty to Children Act, would hold companies accountable regardless of whether they deliberately designed their products to be addictive. *Id.*

especially if done at a state-by-state rate.[139] In the meantime, the Ninth Circuit has cleared a path by denying immunity where plaintiffs regard social media companies in their capacities as products manufacturers.[140]

III. ENTER *LEMMON*

A. Lemmon v. Snap

1. Facts of the Case

Around 7:00 p.m. on May 28, 2017, three young men drove down Cranberry Road in Walworth County, Wisconsin.[141] Jason Davis (age 17) sat behind the wheel, Landen Brown (age 20) rode in the front passenger seat, and Hunter Morby (age 17) rode in the back seat.[142] They careened down the road as fast as 123 mph for several minutes before eventually running off the road and crashing into a tree.[143] The car burst into flames, and all three boys tragically perished.[144]

In the minutes preceding the accident, Landen opened the Snapchat app and used it to see just how fast they were going.[145] Snapchat is a social media platform that allows its users to take photos and videos (snaps) and share them with other users.[146] Snapchat rewards users with various achievements based on the snaps they send but does not disclose how to earn these achievements.[147] Snapchat also provides filters to superimpose over their photos and videos, such as the "Speed Filter," which records and displays the users' "real-life speed" when the user takes the snap.[148] The court noted that many Snapchat users suspected or believed that Snapchat would reward them for taking a snap with the Speed Filter recording a 100 mph or faster speed.[149] Landen

139. *See id.* ("This is a top issue for parents right now.").
140. *See* Lemmon v. Snap, Inc., 995 F.3d 1085, 1093 (9th Cir. 2021) ("The duty to design a reasonably safe product is fully independent of Snap's role in monitoring or publishing third-party content.").
141. *Id.* at 1088.
142. *Id.*
143. *Id.*
144. *Id.*
145. *Id.*
146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.* at 1089. The court recognized that recording a 100 mph or faster speed "is a game for Snap

used the Speed Filter minutes before the fatal accident.[150]

Hunter's and Landen's parents filed a negligent design lawsuit against Snap, alleging that Snapchat should have known that its Speed Filter incentivized young drivers to drive at dangerous speeds.[151] The parents cited a series of news articles about the phenomenon, an online petition, three accidents linked to high-speed snaps, and one other nearly identical lawsuit.[152] They also alleged that Snapchat's warnings to prevent users from using the Speed Filter while driving were ineffective and that "Snap did not remove or restrict access to Snapchat while traveling at dangerous speeds or otherwise properly address the danger it created."[153] The district court granted Snap's motion to dismiss the parents' amended complaint solely based on Section 230 immunity.[154] The Ninth Circuit reversed according to the following reasoning.[155]

2. Analysis of the Decision

The court began by characterizing Section 230 as limited to shielding internet platforms from liability "to the extent their platforms publish third-party content."[156] To determine whether Section 230 immunity applies, the court applied a three-prong test first set forth in *Barnes v. Yahoo!, Inc.*:[157] immunity applies only if Snap is "(1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider."[158]

First, the court classified Snap as an interactive computer service because Snapchat necessarily "enables computer access by multiple users to a computer server"[159] in permitting its users to share photos and videos over the

and many of its users." *Id.*

150. *Id.* at 1088.

151. *Id.* at 1089–90.

152. *Id.* at 1089. *See generally* Maynard v. Snapchat, Inc., 816 S.E.2d 77 (Ga. Ct. App. 2018) (considering another car accident allegedly caused by Snapchat's speed filter).

153. *Lemmon*, 995 F.3d at 1089–90.

154. *Id.* at 1090.

155. *Id.* at 1095.

156. *Id.* at 1090–91.

157. 570 F.3d 1096, 1100–01 (9th Cir. 2009).

158. *Lemmon*, 995 F.3d at 1091 (quoting Dyroff v. Ultimate Software Grp., Inc., 934 F.3d 1093, 1097 (9th Cir. 2019)).

159. 47 U.S.C. § 230(f)(2) (2018).

internet.[160]

Second, the court concluded that the parents' cause of action did not treat Snap as a "publisher or speaker" of third-party content because their claim turned on Snap's design of Snapchat.[161] The court defined "publication" in this context as involving "reviewing, editing, and deciding whether to publish . . . third-party content."[162] The court focused on whether the duty the plaintiffs alleged stemmed from Snap's "status or conduct as a publisher or speaker."[163] The parents' negligent-design legal theory did not rest on treating Snap as a "publisher or speaker" but as a manufacturer with a "duty to exercise due care in supplying products that do not present an unreasonable risk of injury or harm to the public."[164] Furthermore, the fact that Snap allows its users to send user-created content to one another did not detract from how the parents sought to hold Snap liable for designing an unreasonably unsafe product.[165] The court deemed Snap's duty to design a reasonably safe product to be fully independent of its role in monitoring and publishing third-party content.[166] Therefore, Section 230 immunity was unavailable.[167]

Third, the Ninth Circuit also held Section 230 immunity to be unavailable because the parents' negligent design claim did not turn on information provided by a third party.[168] This decision built on recent precedent to offer a new level of clarity regarding internet products liability.[169]

160. *Lemmon*, 995 F.3d at 1091.

161. *Id.*

162. *Id.* (quoting HomeAway.com v. City of Santa Monica, 918 F.3d 676, 681 (9th Cir. 2019).

163. *Id.* (quoting Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1107 (9th Cir. 2009)).

164. *Id.* at 1092 (quoting LEWIS BASS & THOMAS PARKER REDICK, PRODUCTS LIABILITY: DESIGN & MANUFACTURING DEFECTS § 2.5 (2d ed., Sept. 2020 Update)).

165. *Id.*; *see also* Doe v. Internet Brands, Inc., 824 F.3d 846, 849, 854 (9th Cir. 2016) (refusing to bar an aspiring model's claims against a networking website operator for negligently failing to warn her about people using the platform to identify targets for a rape scheme because the claim did not treat the operator as a publisher of content provided by somebody else and therefore was not barred by Section 230).

166. *Lemmon*, 995 F.3d at 1093.

167. *Id.* (citing Maynard v. Snapchat, Inc., 816 S.E.2d 77, 81 (Ga. Ct. App. 2018)).

168. *Id.* (citing *Barnes*, 570 F.3d at 1101).

169. *See infra* Part III.B.

B. Lemmon *in Context: Similar Decisions*

In 2018, the Georgia Court of Appeals considered a remarkably identical case in *Maynard v. Snapchat, Inc.*.[170] There, Plaintiffs, the Maynards, alleged the driver in a serious car accident was using Snapchat's speed filter and driving faster than 100 mph at the time of the crash.[171] The Maynards further alleged that "Snapchat knew that its users could 'use its service in a manner that might distract them from obeying traffic or safety laws'" and that the speed filter "'encourages' dangerous speeding."[172] The trial court applied Section 230 immunity because Snapchat was "merely the publisher of third-party content, not the creator of content."[173] But the court of appeals reversed, recognizing that Snapchat was not entitled to Section 230 immunity because the published content arose out of Snapchat's own application—the speed filter itself—and not content created or posted by third parties.[174] This holding was relatively narrow, focusing primarily on the absence of third-party content, but it helped set the stage for *Lemmon* to further limit Section 230's immunity by isolating internet companies' duty as responsible products manufacturers.[175]

In *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, the Ninth Circuit distinguished Section 230's limitations according to what the internet company developed.[176] As a part of Roommates.com's online forum for people seeking roommates, the site featured a form that required users to disclose personal demographic information such as gender, sexual orientation, and family status before they could use the platform.[177] Plaintiff asserted claims under the Fair Housing Act and related state laws, alleging that Roommates.com forced users to disclose protected information that would be otherwise illegal if used for housing decisions.[178]

The court reasoned that if an internet company "passively displays content that is created entirely by third parties, then it is only a service provider

170. 816 S.E.2d at 77.
171. *Id.* at 79.
172. *Id.*
173. *Id.*
174. *Id.* at 81.
175. Lemmon v. Snap, Inc., 995 F.3d 1085, 1093 (9th Cir. 2021).
176. 521 F.3d 1157, 1166–67 (9th Cir. 2008) (en banc).
177. *Id.* at 1161.
178. *Id.* at 1162–63.

with respect to that content."[179] However, regarding the content that it creates itself, or is responsible in whole or in part for creating or developing, the website is also a content provider and, therefore, not protected by Section 230 immunity.[180] Thus, the Ninth Circuit held that Section 230 did not immunize Roommates.com against claims arising out of the required disclosure of protected information because it helped "develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct."[181]

The *Roommates.com* reasoning clarified that merely "providing *neutral* tools to carry out what may be unlawful or illicit searches does not amount to 'development' for purposes of the immunity exception."[182] This decision significantly shaped the current understanding of liability for content and products that an internet company develops itself.[183]

IV. A SYLLOGISTIC ARGUMENT FOR ENGAGEMENT ALGORITHM PRODUCTS LIABILITY

Aristotle lends us his logical theory of the syllogism to forge ahead.[184] A syllogism consists of two "things supposed" (premises) and what "results of necessity" (a conclusion).[185] Thus, Part IV will follow the syllogistic argument: If companies are liable for harm caused by their products, and if engagement algorithms are products, then internet companies should be liable

179. *Id.* at 1162.

180. *Id.*

181. *Id.* at 1167–68. However, claims arising out of an optional "additional comments" field were barred under Section 230 because the descriptions in this field were optional and did not encourage discriminatory practices. *Id.* at 1174. Although the Ninth Circuit allowed the required disclosure of protected information claims to proceed, it later determined that Roommates.com did not actually violate the Fair Housing Act. *See* Fair Hous. Council of San Fernando Valley v. Roommate.com, LLC, 666 F.3d 1216, 1222 (9th Cir. 2012) ("Because we find that the FHA doesn't apply to the sharing of living units, it follows that it's not unlawful to discriminate in selecting a roommate. As the underlying conduct is not unlawful, Roommate's facilitation of discriminatory roommate searches does not violate the FHA.").

182. *Roommates.com*, 521 F.3d at 1169.

183. *See, e.g.*, Lemmon v. Snap, Inc., 995 F.3d 1085, 1093 (9th Cir. 2021) ("[I]nternet companies remain on the hook when they create or develop their own internet content." (citing *Roommates.com*, 521 F.3d at 1162)).

184. *See* Robin Smith, *Aristotle's Logic*, STAN. ENCYCLOPEDIA OF PHIL., https://plato.stanford.edu/entries/aristotle-logic/#SubLogSyl (Nov. 22, 2022).

185. *Id.*

for harm caused by engagement algorithms.[186]

A. Companies Are Liable for Harm Caused by their Products

To prove strict liability for design defect, a plaintiff must prove each of the following elements:

> [(1)] The defendant sells a product that the plaintiff uses[; (2) t]he defendant is the commercial seller of such a product[; (3) t]he plaintiff suffers an injury[; (4) w]hen the defendant sold the item, the item was defective[; and (5) t]he defect was an actual and proximate cause of the plaintiff's injury.[187]

To show an item is defective, a plaintiff must prove that a reasonable alternative design could have reduced or avoided the foreseeable risks of harm posed by the product.[188]

The typical law classroom examples of products liability include fact patterns about physical products.[189] Software and internet platforms have largely been exempt from the theory of products liability because of the internet exceptionalism championed by Section 230, but the reasoning in *Lemmon* illuminates the greater opportunity for applying this theory to the internet.[190] The Ninth Circuit noted that the claims rested on Snap's "own acts"[191] and were "not predicated on 'information provided by another information content provider.'"[192] This reasoning sets the stage for design defect liability for products that are not mere "neutral tools" that display third-party content the internet company did not develop.[193]

186. *See infra* Sections IV.A–C.

187. *Products Liability*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/products_liability (last visited Feb. 20, 2023).

188. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2(b) (AM. L. INST. 1998).

189. *See, e.g.*, O'Brien v. Muskin Corp., 463 A.2d 298, 302 (N.J. 1983) (finding the manufacturer of an above-ground pool liable for a design defect even though the product complied with modern technological advances).

190. Lemmon v. Snap, Inc., 995 F.3d 1085, 1094 (9th Cir. 2021).

191. *Id.* (citing Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1165 (9th Cir. 2008)).

192. *Id.* at 1094 (citing Barnes v. Yahoo, 570 F.3d 1096, 1101 (9th Cir. 2009)).

193. *See infra* Section IV.B.

B. Engagement Algorithms Are Products, and Not Just "Neutral Tools"

Currently, an internet company enjoys Section 230 immunity if their product is merely a neutral tool, such as when the company "passively display[s]" unlawful content.[194] But where a tool is responsible, in whole or in part, for the creation or development of unlawful content, it is no longer neutral because it functions to bring the company into the role of an information content provider under Section 230's language.[195] According to the Ninth Circuit in *Roommates.com*, an internet company qualifies as an information content provider when it helps to develop unlawful content by reaching beyond generally augmenting content and "contributes materially to the alleged illegality of the conduct."[196] In considering potential liability for engagement algorithms, this reasoning begs the question: Are algorithms neutral tools?[197]

In *Dyroff v. Ultimate Software Group, Inc.*, the Ninth Circuit held that the internet platform defendant's recommender algorithm "amounted to content-neutral functions that did not create a risk of harm."[198] There, the plaintiff's son died from a drug overdose after connecting with a drug dealer through the defendant's internet platform, which allegedly facilitated illegal drug sales.[199] The site recommended groups for users to join based on the content of their posts using machine-learning algorithms.[200] The plaintiff argued that the website operator was an information content provider, as defined by Section 230, because its recommendation functions were "specifically designed to make subjective, editorial decisions about users based on their posts."[201] The court rejected this argument and held that by recommending user groups and sending notifications, the website acted only as a publisher of others' content.[202]

It is inappropriate to classify modern social media engagement algorithms

194. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1174 (9th Cir. 2008).

195. 47 U.S.C. § 230(f)(3) (2018).

196. *Roommates.com*, 521 F.3d at 1167–68.

197. *See, e.g.*, Complaint at 20, Cohen v. Facebook, Inc., 1:16-cv-04453 (E.D.N.Y. Aug. 10, 2016). "Facebook's active involvement in making connections between its users . . . renders it as far more than a neutral and passive bulletin board for information provided by others. Its active role in making connections . . . requires that it be held accountable for its actions." *Id.*

198. 934 F.3d 1093, 1100 (9th Cir. 2019).

199. *Id.* at 1094–95.

200. *Id.*

201. *Id.* at 1096.

202. *Id.* at 1098 ("These functions—recommendations and notifications—are tools meant to facilitate the communication and content of others. They are not content in and of themselves.").

as neutral tools because they function beyond passive publishing and recommending—they become products in and of themselves that materially contribute to harm.[203] Unlike the simple recommender tool in the *Dyroff* case that merely suggested groups to join based on user interests, social media companies specifically engineer algorithms to addict users through harmful methods.[204]

Social media platforms connect our public communication sphere, yet the companies that operate these platforms are answerable only to their profit margins, not to the public.[205] While they often advertise themselves as free to consumers, social media companies gain revenue by keeping users engaged with their platforms.[206] The longer users stay engaged, the more exposure advertisements receive, creating a profit incentive.[207] And because inflammatory and socially-harmful content is so engaging, it can be "economically valuable to platform owners while posing relatively little economic harm to their public image or brand name."[208]

Social media platforms curate their news feeds to be interesting and relatable to users to keep them "engaged for as long and as frequently as possible."[209] To accomplish this, social media companies utilize data about users' preferences to predict what they will find interesting.[210] Algorithms do the heavy lifting in analyzing enormous amounts of raw user data to predict user interests.[211] In its most basic function, an algorithm is simply a "step-by-step procedure to accomplish a goal,"[212] analyzing information, prioritizing

203. *See* Catherine Tremble, *Wild Westworld: Section 230 of the CDA and Social Networks' Use of Machine-Learning Algorithms*, 86 FORDHAM L. REV. 825, 827 (2017) ("Machine-learning algorithms' subtle but pervasive influence alters human behavior and, to a certain extent, the human experience.").

204. *See id.*; *Dyroff*, 934 F.3d at 1095.

205. *See* Kim, *supra* note 11, at 147 ("At their core, social media platforms are businesses."); *see also* Brené Brown, *Free Speech, Misinformation, and the Case for Nuance with Ben Wizner*, SPOTIFY, at 49:48 (Feb. 9, 2022), https://brenebrown.com/podcast/free-speech-misinformation-and-the-case-for-nuance/#listen ("These are institutions that are not answerable to the public, they are answerable to their shareholders and bottom line.").

206. *See* Kim, *supra* note 11, at 147.

207. *Id.*; *see also* Alfred Lua, *How the Instagram Algorithm Works in 2021: Everything You Need to Know,* BUFFER (Feb. 16, 2021), https://blog.bufferapp.com/instagram-algorithm [https://perma.cc/L5PD-76JG].

208. Smith & Van Alstyne, *supra* note 22.

209. Kim, *supra* note 11, at 148.

210. *Id.*

211. *Id.* at 149.

212. Zakon, *supra* note 22, at 1111; *see also* G. MICHAEL SCHNEIDER & JUDITH L. GERSTING,

factors, and predicting outcomes along the way.[213]

First, as the algorithm analyzes the accumulated raw user data, it categorizes information to reveal patterns about what a user likes to see.[214] "The more frequent the engagement, the stronger the association the algorithm will make between the user and that content."[215] Even when users are more passive, and do not click, share, comment, or like a post, algorithms can measure interest by tracking the amount of time a user keeps a post on the screen before scrolling on.[216] Rumors about Facebook and other prominent social media applications listening to user conversations have been largely debunked, but these platforms do use "sophisticated demographic and location data" to supplement user information to create a very accurate marketing profile.[217]

Using the data as a guide, the algorithm then creates a pool of content that matches the patterned interests of the user and ranks the content based on its appeal.[218] Algorithms can use various multipliers to boost certain content, such as posts from close friends or announcements regarding major life events.[219] Every detail is carefully oriented to maximize engagement, and the results are fed back into the algorithm to increase the accuracy of its prediction.[220] "Using an iterative process of trial and error over time, recommender systems learn which highly personalized suggestions will delight users most."[221]

These highly effective engagement algorithms are more complex than

---

INVITATION TO COMPUTER SCIENCE 11–17 (8th ed. 2018) (breaking down basic algorithmic elements and functions).

213. Kim, *supra* note 11, at 149.

214. *Id.*

215. *Id.*

216. *Id.* at 150.

217. Jefferson Graham, *Is Facebook Listening to Me? Why Those Ads Appear After You Talk About Things*, USA TODAY, https://www.usatoday.com/story/tech/talkingtech/2019/06/27/does-facebook-listen-to-your-conversations/1478468001/ (June 28, 2019, 5:18 PM) ("'Facebook is eavesdropping on you,' says Jamie Court, the president of Los Angeles-based Consumer Watchdog nonprofit. 'It's just in a different way. . . . It's like they're stalking you, . . . They put all sorts of circumstantial evidence together, and you're marketed to as if they're listening to your conversations.'").

218. *See* Kim, *supra* note 11, at 150 ("After the algorithm creates a pool of potentially interesting content for a user, the algorithm gives each content a rank based on its appeal to the user.").

219. *Id.* ("Within the pool, the algorithm may boost the rank of certain content, such as actions by close friends, by applying a multiplier.").

220. *See* Zakon, *supra* note 22, at 1113 ("Once the system selects a permutation of choices to show, it observes the user's behavior and evolves independently via reinforcement learning paradigms.").

221. *Id.*

Snapchat's speed filter at issue in *Lemmon*, but both are profit-yielding, intentionally developed products that the companies provide to the public marketplace.[222] Snapchat attracted the boys from *Lemmon* to its platform with its speed filter, just as social media companies entice users with engagement algorithms.[223] Therefore, liability should apply in both scenarios when the products are harmful.

C. Internet Companies Should be Liable for Harm Caused by Engagement Algorithms

With the premises established, a gap in the immunity labyrinth's wall "results of necessity."[224] Section 230 immunity should not protect internet companies in their capacity as algorithm manufacturers when their tools cause harm.[225] A design defect theory of liability could apply to two types of engagement algorithm "defects": inattentional blindness and feedback loops, "both of which are collateral consequences of the 'arms race for attention.'"[226] Inattentional blindness occurs when developers focus the algorithm on a specific engagement goal and overlook user well-being.[227] A feedback loop occurs when an engagement algorithm "relies on recommendations it has already made" so that the output becomes the input.[228] Feedback loops result in repeated exposure to a limited type of content, which becomes harmful when that content is extreme.[229] As previously noted, for plaintiffs to succeed in a design defect claim, they must demonstrate the platform could have avoided the harm at issue by adopting a reasonable alternative design.[230] One viable

222. Kim, *supra* note 11, at 148–51 (reviewing the business purpose for using algorithms to attract users, as well as the mechanics that companies have developed to accomplish this goal); Lemmon v. Snap, Inc., 995 F.3d 1085, 1088 (9th Cir. 2021).

223. *See Lemmon*, 995 F.3d at 1088.

224. Smith, *supra* note 187.

225. *See* Tremble, *supra* note 206, at 868 ("[A]lgorithmic technology that springs forth distinct from user-generated content and is powerful enough to influence human behavior should be given due consideration in a revised framework, instead of obtaining customary immunity.").

226. Zakon, *supra* note 22, at 1128 (quoting RECOMMENDER SYSTEMS HANDBOOK 5 (Francesco Ricci et al. eds., 2011).

227. *Id.*

228. *Id.*; *see also* Swathi Meenaskhi Sadagopan, *Feedback Loops and Echo Chambers: How Algorithms Amplify Viewpoints*, CONVERSATION (Feb. 4, 2019, 4:18 PM), http://theconversation.com/feedback-loops-and-echo-chambers-how-algorithms-amplifyviewpoints-107935.

229. Zakon, *supra* note 22, at 1128–29.

230. *See* RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2(b) (AM. L. INST. 1998).

alternative design option would be modifying an algorithm's objective function "to both explicitly consider user welfare and mitigate the effects of hyper-personalization through aggregation."[231] The harm stemming from the addictive and isolating effects of engagement algorithms has been well documented.[232]

1. Harm to Individuals Caused by Engagement Algorithms

a. Inattentional Blindness

What is the cost of engineering social media to be as engaging as possible?[233] Social media companies' efforts have certainly not been in vain, as social media use has increased drastically over the past decade.[234] Only five percent of American adults used at least one social media platform in 2005, compared with seventy-two percent in 2019.[235] The top social media platforms combine to cover billions of active users.[236] Vulnerable populations, including young children and those with pre-existing mental health conditions, are among the most frequent users.[237] A 2018 study revealed that ninety-five percent of teenagers use a smartphone, and forty-five percent reported that they were online "almost constantly."[238]

Several studies have linked adverse mental health effects to social media

231. Zakon, *supra* note 22, at 1130.

232. *See infra* Section IV.B.

233. *See* Clodagh O'Brien, *How Do Social Media Algorithms Work?*, DIGIT. MKTG. INST. (Jan. 19, 2022), https://digitalmarketinginstitute.com/blog/how-do-social-media-algorithms-work (reviewing how the Facebook, Pinterest, LinkedIn, Twitter, and Instagram algorithms prioritize various factors to make their platforms as engaging as possible to users).

234. *Social Media Fact Sheet*, PEW RSCH. CTR. (June 12, 2019), https://www.pewinternet.org/fact-sheet/social-media/ [https://perma.cc/Z7GL-RUU8].

235. *Id.*

236. *See* Karl, *The 15 Biggest Social Media Sites and Apps*, DREAMGROW (Jan. 7, 2023), https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/#The_Top_15_Social_Media_Sites_and_Apps_by_Active_Users (listing Facebook at 2.74 billion active users; YouTube at 2.29 billion; Instagram at 1.22 billion; TikTok at 689 million; Telegram at 500 million; and Snapchat at 498 million).

237. Aksha M. Memon et al., *The Role of Online Social Networking on Deliberate Self-Harm and Suicidality in Adolescents: A Systemized Review of Literature*, 60(4) INDIAN J. PSYCHIATRY 384, 390 (2018).

238. Monica Anderson & Jingjing Jiang, *Teens, Social Media & Technology 2018*, PEW RSCH. CTR. (May 31, 2018), https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/ [https://perma.cc/3GM2-TMCY].

addiction, ranging from "body image issues to depression and suicide."[239] Social media companies design their engagement algorithms to "trap users in a cycle of dependance . . . exacerbate[ing] these harms."[240] People using social networks excessively suffer from a sort of "Facebook Addiction Disorder" with addiction criteria behavioral symptoms such as "neglect of personal life, mental preoccupation, escapism, mood modifying experiences, tolerance and concealing the addictive behavior."[241] Studies show a withdrawal effect with psychological and physiological symptoms when people stop using the internet and social media.[242] Another study found that Facebook use was linked to less moment-to-moment happiness and less life satisfaction,[243] and yet another study linked social media use across eleven major platforms to greater "perceived social isolation."[244] Perhaps most unsettling is a series of internal studies done within Facebook showing that the company is acutely aware of the harm it causes its users.[245] One such study on Instagram, which Facebook

239. Zakon, *supra* note 22, at 1116.

240. *Id.*; *see also* Catherine Price, *Trapped - The Secret Ways Social Media Is Built to Be Addictive (and What You Can Do to Fight Back)*, SCI. FOCUS (Oct. 29, 2018, 8:00 AM), https://www.sciencefocus.com/future-technology/trapped-the-secret-ways-social-media-is-built-to-be-addictive-and-what-you-can-do-to-fight-back/ [https://perma.cc/MF59-K77H].

241. Daria J. Kuss & Mark D. Griffiths, *Online Social Networking and Addiction—A Review of the Psychological Literature*, 8 INT'L J. OF ENV'T RSCH. AND PUB. HEALTH 3528, 3529 (2011).

242. PHIL REED ET AL., DIFFERENTIAL PHYSIOLOGICAL CHANGES FOLLOWING INTERNET EXPOSURE IN HIGHER AND LOWER PROBLEM-ATIC INTERNET USERS (Mazza ed.,2017).

243. ETHAN KROSS ET AL., FACEBOOK USE PREDICTS DECLINES IN SUBJECTIVE WELL-BEING IN YOUNG ADULTS (Sueur ed., 2013) ("On the surface, Facebook provides an invaluable resource for fulfilling such needs by allowing people to instantly connect. Rather than enhancing well-being, as frequent interactions with supportive 'offline' social networks powerfully do, the current findings demonstrate that interacting with Facebook may predict the opposite result for young adults—it may undermine it.").

244. Brian A. Primack, M.D. et al., *Social Media Use and Perceived Social Isolation Among Young Adults in the U.S.*, 53 AM. J. OF PREVENTATIVE MED. 1, 1 (2017) (study included engagement with Facebook, Twitter, Google+, YouTube, LinkedIn, Instagram, Pinterest, Tumblr, Vine, Snapchat, and Reddit).

245. Georgia Wells, Jeff Horwitz & Deepa Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, WALL ST. J. (Sept. 14, 2021, 7:59 AM), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739?mod=article_inline ("The Instagram documents form part of a trove of internal communications reviewed by the Journal, on areas including teen mental health, political discourse and human trafficking. They offer an unparalleled picture of how Facebook is acutely aware that the products and systems central to its business success routinely fail."); *see also* Jeff Horwitz, *The Facebook Whistleblower, Frances Haugen, Says She Wants to Fix the Company, Not Harm It*, WALL ST. J. (Oct. 3, 2021, 7:36 PM), https://www.wsj.com/articles/facebook-whistleblower-frances-haugen-says-she-wants-to-fix-the-company-not-harm-it-11633304122?mod=article_inline (describing how

owns, stated, "[w]e make body image issues worse for one in three teen girls."[246]

Indeed, social media seems to be particularly damaging for teen girls.[247] Social media "displaces other forms of interactions among teens" and intensifies the "worst parts of middle school and glossy women's magazines."[248] Gen Z, the generation born after 1996, has experienced a drastic increase in major depressive episodes since the early 2010s, and researchers have found corresponding increases in suicide and self-harm, particularly for girls.[249] Tragically, the rate of hospital admissions for self-harm doubled for girls ages ten to fourteen between 2010 and 2014.[250] Correlative data, as well as self-reported evidence, support the connection between the mental health epidemic and social media addiction.[251] "If Americans do nothing until researchers can show beyond a reasonable doubt that [social media companies] are hurting teen girls, these platforms might never be held accountable, and the harm could continue indefinitely. The preponderance of the evidence now available is disturbing enough to warrant action."[252]

b. Feedback Loops

Feedback loops, where an engagement algorithm relies on its own recommendations, result in echo chambers and filter bubbles.[253] An echo chamber is the effect of a user's "interest being positively or negatively reinforced by

whistleblower Frances Haugen leaked thousands of internal documents to journalists with the goal of exposing how the social media giant consistently put profits over people).

246. Wells et al., *supra* note 245.

247. Jonathan Haidt, *The Dangerous Experiment on Teen Girls*, ATLANTIC (Nov. 21, 2021), https://www.theatlantic.com/ideas/archive/2021/11/facebooks-dangerous-experiment-teen-girls/620767/?mc_cid=fbc16f73b2&mc_eid=0f7ca0d7c2.

248. *Id.* Instagram is particularly damaging in this regard, because it "puts the size of their friend group on public display, and subjects their physical appearance to the hard metrics of likes and comment counts." *Id.*

249. *Id.*

250. *Id.*

251. *Id.* Instagram, Snapchat, and Facebook scored as the most harmful when British researchers asked 1,500 teens to rate how social media platforms affected their anxiety, loneliness, body image, and sleep. *Instagram Ranked Worst for Young People's Mental Health*, ROYAL SOC'Y FOR PUB. HEALTH (May 19, 2017), https://www.rsph.org.uk/about-us/news/instagram-ranked-worst-for-young-people-s-mental-health.html.

252. Haidt, *supra* note 247.

253. RAY JIANG ET AL., ASS'N FOR THE ADVANCEMENT OF A.I., DEGENERATE FEEDBACK LOOPS IN RECOMMENDER SYSTEMS 383 (2019).

repeated exposure to a certain item or category of items."[254] A filter bubble refers to "the fact that recommender systems select limited content to serve users online."[255]

Another study conducted by Facebook Research examined the impact of algorithms on the spread of negativity on the site.[256] There, researchers adjusted content algorithms to manipulate user newsfeeds, removing positive posts from some and negative posts from others, and found that people who saw more negative posts in their feed became more negative in their own posts.[257]

Facebook's internal research demonstrates further harmful effects, which was leaked to the press via a whistleblower.[258] The documents reveal that Facebook changed its engagement algorithm in 2018 to reverse a decline in engagement and to encourage more original posting.[259] Mark Zuckerberg announced at the time that he was shifting the Facebook product managers' goal from helping people find relevant content to helping them interact more with friends and family.[260] The new algorithm changed the rewarded posts by recommending them more if they garnered more comments and emoji reactions, which were deemed more meaningful than likes.[261] Facebook's own research shows that "the new algorithm's heavy weighting of reshared material . . . made the angry voices louder."[262] "Misinformation, toxicity, and violent content are inordinately prevalent among reshares," the research found.[263]

254. *Id.*
255. *Id.*
256. Zakon, *supra* note 22, at 1117.
257. *Id.*
258. Hagey & Horwitz, *supra* note 13; Horwitz*, supra* note 245 ("[The whistleblower found] that despite numerous initiatives, Facebook didn't address or make public what it knew about its platforms' ill effects.").
259. Hagey & Horwitz, *supra* note 13.
260. *Id.*
261. *Id.*
262. *Id.*
263. *Id.*

2. Harm to Society Caused by Engagement Algorithms

Engagement algorithms also have damaging societal effects on a macro level.[264] The same internal Facebook research found that engagement-maximizing algorithm changes had an international political impact because political parties "now have an incentive . . . to create posts that rack up comments and shares—often by tapping into anger—to get exposure in users' feeds."[265] "[H]arsh attacks on [political] opponents net the highest engagement," and political parties vying for positions will "use what works."[266] In this way, social media engagement algorithms recommend increasingly inflammatory and narrow content in order to keep users' attention.[267] One scholar noted YouTube's "algorithm seems to have concluded that people are drawn to content that is more extreme than what they started with—or to incendiary content in general."[268]

These societal threats are compounded in magnitude by ongoing cybersecurity concerns, especially in the context of democratic elections.[269] Troll farms, which are "professionalized groups that work in a coordinated fashion to post provocative content, often propaganda, to social networks," reached 140 million Americans per month on Facebook before the 2020 presidential election.[270] Seventy-five percent of those users had never followed the troll

264. *Id.* The "Political effect" section of the article explores far-reaching political impacts of algorithms on social media. *See id.*

265. *Id.* Facebook researchers wrote in an April 2019 internal report on Polish political parties: "One party's social media management team estimates that they have shifted the proportion of their posts from 50/50 positive/negative to 80% negative, explicitly as a function of the change to the algorithm." *Id.*

266. *Id.*

267. *See* Renee DiResta, *Up Next: A Better Recommendation System*, WIRED (Apr. 11, 2018, 11:00 AM), https://www.wired.com/story/creating-ethical-recommendation-engines/ [https://perma.cc/HRW6-WKWQ] ("The systems don't actually understand the content, they just return what they predict will keep us clicking. That's because their primary function is to help achieve one or two specific key performance indicators (KPIs) chosen by the company.").

268. Zeynep Tufekci, *YouTube, the Great Radicalizer*, N.Y. TIMES (Mar. 10, 2018), https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html [https://perma.cc/TW6B-83N8].

269. Karen Hao, *Troll Farms Reached 140 Million Americans a Month on Facebook Before 2020 Election, Internal Report Shows*, MIT TECH. REV. (Sept. 16, 2021), https://www.technologyreview.com/2021/09/16/1035851/facebook-troll-farms-report-us-2020-election/.

270. *Id.* "This is not normal. This is not healthy. . . . We have empowered inauthentic actors to accumulate huge followings for largely unknown purposes . . . The fact that actors with possible ties to the [Kremlin-backed Internet Research Agency] have access to huge audience numbers in the same demographic groups targeted by the IRA poses an enormous risk to the US 2020 election." *Id.*

farm pages, but "[t]hey were seeing the content because Facebook's content-recommendation system had pushed it into their news feeds."[271] Facebook's internal report on the matter revealed "around 15,000 Facebook pages with a majority US audience were being run out of Kosovo and Macedonia," which were known bad actors in the 2016 election.[272] Alarmingly, these troll farm pages included all fifteen of the largest Christian–American Facebook pages, ten of the top fifteen African-American pages, four of the top Native American pages, and the fifth-largest women's page.[273] Engagement algorithms create "distorted, economic incentives" and enable bad actors to weaponize social media platforms to interfere with the democratic process by artificially swaying public opinion.[274]

Then, there is the gradual, yet fundamental changing of our minds to consider.[275] "[O]ur neural circuits—whether they're involved in feeling, seeing, hearing, moving, thinking, learning, perceiving, or remembering—are subject to change."[276] Our brains use this "neuroplasticity" to fine-tune their operations by optimizing routine activities to be more efficient while pruning away unused circuits.[277] The human brain, which once embraced the "solitary, single-minded concentration" of the book,[278] has shifted to move quickly through

271. *Id.* "Instead of users choosing to receive content from these actors, it is our platform that is choosing to give [these troll farms] an enormous reach," wrote the internal report's author, Jeff Allen, a former senior-level data scientist at Facebook. *Id.*

272. *Id.*

273. *Id.* Specifically, top troll farm pages included:

> [T]he largest Christian American page on Facebook, 20 times larger than the next largest—reaching 75 million US users monthly, 95% of whom had never followed any of the pages[,] . . . the largest African-American page on Facebook, three times larger than the next largest—reaching 30 million US users monthly, 85% of whom had never followed any of the pages[,] . . . the second-largest Native American page on Facebook, reaching 400,000 users monthly, 90% of whom had never followed any of the pages[,] . . . [and] the fifth-largest women's page on Facebook, reaching 60 million US users monthly, 90% of whom had never followed any of the pages.

Id. "Our platform has given the largest voice in the Christian American community to a handful of bad actors, who, based on their media production practices, have never been to church." *Id.* "Our platform has given the largest voice in the African American community to a handful of bad actors, who, based on their media production practices, have never had an interaction with an African American." *Id.*

274. *Id.*

275. *See generally* NICHOLAS CARR, THE SHALLOWS: WHAT THE INTERNET IS DOING TO OUR BRAINS (W.W. Norton & Co. 2011) (discussing the internet's impact on our neural processing).

276. *Id.* at 26.

277. *Id.* at 34.

278. *Id.* at 114.

the internet's "cacophony of stimuli," short-circuiting our thoughts and "preventing our minds from thinking either deeply or creatively."[279] Our addiction to distraction is profitable for social media companies, but it may be costing us some of our humanity.[280]

Many of these macro effects stretch beyond the causal connection needed in a viable products liability cause of action.[281] But recognizing engagement algorithms' far-reaching impact is integral to this conversation to inform our understanding of algorithmic harm if we are to accomplish effective reform.[282] In the meantime, it is helpful to recognize in these divided times that people who fiercely oppose our viewpoints may not be wicked or unintelligent but simply "trapped in a different algorithm than [we] are."[283]

V. CONCLUSION

Individuals harmed by engagement algorithms currently have no recourse under Section 230's broad immunity, but courts addressing claims that treat internet companies in their capacities as product developers should follow *Lemmon*'s example and hold that CDA immunity does not apply.[284] Social media companies act as information content providers, not in a publishing capacity, when they employ personalized engagement algorithms to addict users.[285] Even without legislatively reforming the Communications Decency Act, this means that internet companies should not be shielded by Section 230 immunity when claims address them in their capacity as the manufacturer of an unreasonably unsafe product.[286]

The harms addressed in this Comment are on the rise and projected to

279. *Id.* at 119. "Our brains turn into simple signal-processing units, quickly shepherding information into consciousness and then back out again." *Id.*

280. *See* NEIL POSTMAN, AMUSING OURSELVES TO DEATH: PUBLIC DISCOURSE IN THE AGE OF SHOW BUSINESS, 155–56 (Penguin Publishing Group 2005) (1985) ("When a population becomes distracted by trivia, when cultural life is redefined as a perpetual round of entertainments, when serious public conversation becomes a form of baby-talk, when, in short, a people become an audience and their public business a vaudeville act, then a nation finds itself at risk; culture-death is a clear possibility.").

281. RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2(b) (AM. L. INST. 1998).

282. *See supra* Section IV.B.

283. AZIZ ANSARI: NIGHTCLUB COMEDIAN (Netflix 2022).

284. *See supra* Section III.A.2 (discussing the analysis in *Lemmon*).

285. Zakon, *supra* note 22, at 1133, 1135 (discussing the inapplicability of products liability publisher immunity to social media platforms).

286. *See supra* Section IV.C.

increase in a future where social media will likely be even more ubiquitous in the human experience.[287] Projects like Facebook's metaverse will continue to replace human interaction with simulated stimulation and employ new versions of engagement algorithms to hook users in.[288] The answer is surely not to embrace a purely Luddite resistance or ignore the internet's undeniable benefits.[289] Rather, the evidence before us calls us to engage thoughtfully, hold accountable those who exploit technology for profit in a way that causes harm and push for reform that expressly protects individual and societal well-being.

While our statutory labyrinth could use a redesign—perhaps around the common law duty of care—cases like *Lemmon* show us that there may be a ball of string in products liability to guide a way through the broad Section 230 immunity.

Tyler Lisea*

287. *See* S. Dixon, *Global Social Network Penetration 2018-2027*, STATISTA (Feb. 13, 2023) https://www.statista.com/statistics/260811/social-network-penetration-worldwide/#statisticContainer. "In 2021, approximately 56 percent of the global population were social media users. This share is projected to increase to 74 percent of the global population by 2026." *Id.*

288. *See* META, https://about.facebook.com/meta/ (last visited Feb. 2, 2023); Mike Isaac, *'Operating With Increased Intensity': Zuckerberg Leads Meta Into Next Phase*, N.Y. TIMES (July 26, 2022), https://www.nytimes.com/2022/07/26/technology/zuckerberg-meta-facebook-earnings.html ("Meta has been investing heavily in video and discovery, aiming to beef up its artificial intelligence and to improve 'discovery algorithms' that suggest engaging content to users without them having to work to find it.").

289. *See* Tom de Castella, *Are You a Luddite?*, BBC NEWS MAG. (Apr. 20, 2012), https://www.bbc.com/news/magazine-17770171 (reviewing the history of how a weaver uprising—inspired by the fabled King Ludd—against new automated looms in 1811 coined the colloquial term for technophobe).

* J.D. 2023, Pepperdine Caruso School of Law; B.A. 2015, Westmont College. I would first like to thank my beloved wife, Brittany Lisea, for seeing potential in me and loving me into actualizing it. Thank you to my parents, Scott and Jamie Lisea, for your consistent votes of confidence. I am indebted to my undergraduate professors Deborah Dunn, Omedi Ochieng, and Greg Spencer for their patient instruction and for instilling in me a passion for rhetoric and a critical eye. Thank you, Lauren Elvik, my Note & Comment Editor, for your insight and guidance. Finally, thank you to the clerk that oversaw my judicial externship, Catherine Hegdale, for ruthlessly and benevolently leveling up my writing skills through many redline edits.

***