2018

# Intermediary Design Duties

Olivier Sylvain
*Fordham University School of Law*, sylvain@law.fordham.edu

CONNECTICUT
LAW REVIEW

VOLUME 50 MARCH 2018 NUMBER 1

## Article

# Intermediary Design Duties

OLIVIER SYLVAIN

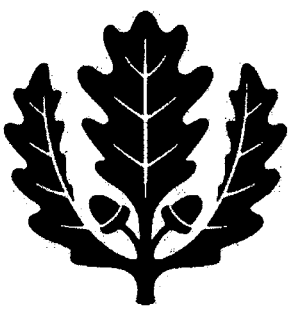
*Online social networking applications and marketplaces enable users to discover ideas, people, places, and products. The companies behind these services purport to be little more than the conduits through which users socialize and transact business. It is on this premise that, pursuant to the Communications Decency Act (CDA), courts are reluctant to impose liability on intermediaries for their users' illegal online conduct. In spite of language in the statute that would limit the safe harbor to intermediaries that voluntarily moderate users' content and behavior, courts today refrain from granting immunity only in cases in which intermediaries "materially contribute" to illegal online conduct. This has proven to be a very high juridical bar for plaintiffs to clear and a very generous protection for defendant providers.*

*This doctrine rests on an outdated view of how most online intermediaries do business. Today, the largest online companies do not merely host and relay messages, uninterested in what their users say or do. They use behavioral and content data to engineer online experiences in ways that are unrelated to the charming interest in making connections. Some of the most successful companies, moreover, collect, analyze, sort, and repackage user data for publication in ancillary and secondary markets. This is how the CDA immunity doctrine, first developed by the courts two decades ago, is ill-suited to the world today. Online intermediaries are now aggressively exploiting user content in ways that the doctrine does not fully acknowledge, leaving public law priorities and consumer protections underenforced. Vulnerable people and historically subordinated groups have the most to lose under this approach.*

*This Article proposes a reform that is adapted to online intermediaries' outsized influence today. It proposes that courts scrutinize the manner in which providers in each case elicit user content and the extent to which they exploit that data in secondary or ancillary markets. Following this more searching approach, courts will return the doctrine to its roots in the language and purpose of the CDA: to shield intermediaries from liability for third-party online conduct only to the extent they operate as either true conduits of user content.*

## ARTICLE CONTENTS





# Intermediary Design Duties

OLIVIER SYLVAIN *

## INTRODUCTION

Online social networking applications and marketplaces enable users to discover ideas, people, places, and products that they would never find otherwise. The companies behind these applications purport to do little more than offer the "tools" for obtaining "information about what's going on in the world."[1] Policymakers, courts, and legal scholars generally agree with this view.[2] They tend to see video sharing applications like YouTube,

---

* Associate Professor of Law, Fordham Law School. I am grateful to the following colleagues and friends for support and helpful comments during the drafting of this Article: Jim Brudney, Danielle Citron, Nestor Davidson, Mary Ann Franks, Eric Goldman, Rachel Goodman, Abner Greene, Jameel Jaffer, Olati Johnson, Joe Landau, Ron Lazebnik, Jae Lee, Ethan Leib, Robin Lenhardt, Frank Pasquale, Mark Patterson, Kimani Paul-Emile, David Pozen, Joel Reidenberg, Ian Weinstein, and Benjamin Zipursky. I am indebted to Michael Risch and all participants of the February 2017 Lastowka Cyberlaw Conference at Villanova School of Law for having the patience to review an early draft of Part II. Participants in the Fordham Law School Center on Race, Law, and Justice Colloquium series provided important insights that have improved the piece. Jocelyn Sagherian of the Fordham law library provided invaluable research support. Meredith Cusick and Eric Hornbeck, my research assistants, were reliable, industrious, and creative in their support of my work on this project.

[1] Christina Passariello, *Facebook: Media Company or Technology Platform?*, WALL. ST. J. (Oct. 30, 2016, 10:22 PM), https://www.wsj.com/articles/facebook-media-company-or-technology-platform-1477880520. *See also* Mathew Ingram, *Facebook Denies It's a Media Outlet, But Many Users Disagree*, FORTUNE (Feb. 9, 2017), http://fortune.com/2017/02/09/facebook-study-news/ (reporting that Facebook resists being labeled as a media company, though many users use Facebook as a news outlet); Sam Schechner, *Uber's 'Not a Taxi Company' Defense on Trial in EU*, WALL ST. J. (Nov. 29, 2016), https://www.wsj.com/articles/ubers-not-a-taxi-company-defense-on-trial-in-eu-1480427094 (internal quotation marks omitted) (explaining Uber's argument that it is not a "transportation company" and is instead "an information society services provider that matches drivers with passengers").

[2] *See* Huon v. Denton, 841 F.3d 733, 741 (7th Cir. 2016) (holding that "a company like Gawker [Media] cannot be considered the publisher of information simply because the company hosts an online forum for third-party users to submit comments."); Zeran v. America Online, Inc., 129 F.3d 327, 330–32 (4th Cir. 1997) (holding that America Online, Inc. is a publisher of information, not a distributor such as a "traditional news vendor[] or book seller[]," and is therefore, under 47 U.S.C. § 230(c)(1), immune to causes of action "that would make service providers liable for information originating with a third-party user of the service"). Scholars have noted that social networking sites, such as Facebook, should be considered "publishers" of the content posted by third parties, in order to prevent a chilling effect on internet free speech. *See, e.g.*, Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 148 (2008) (explaining that 47 U.S.C. § 230, the Communications Decency Act, was passed to prevent a "chilling effect on Internet speech" that would result from imposing liability on internet intermediaries for the statements of third parties); Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 28–29 (2006) (discussing Free Speech implications in holding intermediaries responsible for the statements of third parties and noting that "intermediaries have a peculiarly fragile commitment to the speech that they facilitate . . . . [I]n many

social networking applications like Facebook, ride hailing mobile services like Uber, and short-term homestay marketplaces like Airbnb as the "conduits" through which end users communicate, socialize, and transact business.[3]

One can be forgiven for holding this view. These applications facilitate a variety of useful interactions. It is in this vein that courts today generally conclude that ostensibly passive online intermediaries are immune from liability for their users' online conduct and content.[4] Citing the Communications Decency Act (CDA), courts hold that intermediaries may only be liable if they "materially contribute" to the illegal online conduct and content of their users.[5] Courts reason that online entrepreneurship and speech would be chilled if providers bore the costly burden of policing their many users' online conduct.[6]

This doctrine rests on an outdated view of how most service providers do business. Today, most providers do not simply relay messages in the charming interest of sharing ideas or making connections, uninterested in what users say or do. The most popular applications today collect,

---

situations an intermediary . . . cannot capture the full value of speech, but can easily avoid potential liability by simply declining to carry speech that could raise problems."); Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 991, 998–99, 1006–07, 1009, 1015–16 (2008) (looking favorably upon the Communications Decency Act's efforts to limit an internet intermediary's liability for the statements of its users, while also arguing that the CDA should limit an intermediary's ability to remove content and freely restrict the free speech of its users); Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293, 294, 300 (2011) (noting that websites such as message boards are simply "internet intermediaries" and that imposing liability for harmful or offensive speech on them may cause them to "block or eliminate too much content, including content that might be both lawful and socially desirable").

[3] Fair Hous. Council of San Fernando Valley v. Roomates.Com, LLC, 521 F.3d 1157, 1167 (9th Cir. 2008). *See also* Guy Pessach, *Deconstructing Disintermediation: A Skeptical Copyright Perspective*, 31 CARDOZO ARTS & ENT. L.J. 833, 842 (2013) (referring to "[s]earch engines" such as Google and Yahoo, "content sharing platforms" such as Youtube, "social networks" such as Facebook, and "online vendors" such as Airbnb, Uber, and Amazon as "content conduits and content retrieval mechanisms").

[4] *See Huon*, 841 F.3d at 741–42 (holding that an internet intermediary is immune from liability for defamation if it did not create or actively participate in posting the defamatory content); FTC v. Accusearch Inc., 570 F.3d 1187, 1199 (10th Cir. 2009) ("[T]o be 'responsible' for the development of offensive content, one must be more than a neutral conduit for that content."); *Fair Hous. Council of San Fernando Valley*, 521 F.3d at 1162 ("Section 230 of the CDA immunizes providers of interactive computer services against liability arising from content created by third parties . . . . This grant of immunity applies only if the interactive computer service provider is not also an information content provider . . . . A website operator can be both a service provider and a content provider: If it passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content." (internal footnotes and quotation marks omitted)). Congress, when drafting the CDA, distinguished "interactive computer service[s]," which are immune from liability for the postings of third parties, from "information content providers." *See* 47 U.S.C. §§ 230(c)(1), (f)(3) (1998) (defining "information content providers" as persons or entities that are "responsible, in whole or in part, for the creation and development of information").

[5] Jones v. Dirty World Entm't Recordings, 755 F.3d 398, 412, 415 (6th Cir. 2014).

[6] *Id.*

exhaustively analyze, sort, reconfigure, and repurpose customer information for commercial gain.[7] They rely on proprietary "black box" technologies to recommend products, services, and connections specifically targeted to each user.[8] They employ techniques that keep users yearning for more.[9] Sometimes, their designs are so deeply affecting that they transform the ways in which people talk about experiences in the physical world.[10]

More than this, the companies behind the largest social media applications profit from their extraordinary stores of users' data.[11] While these companies arguably rely on aggregate user information to enhance the online experience for everyone, they, at the same time, also exploit that data in other information markets. Thus, today, online intermediaries do not simply make new connections where none existed before. They commercialize their users' data.

Profits, of course, are not unlawful. They are sometimes a relatively reliable measure of a company's commercial success in the United States.

---

[7] *See, e.g.*, Julia Angwin & Jeremy Singer-Vine, *Selling You on Facebook*, WALL ST. J. (April 7, 2012), https://www.wsj.com/articles/SB10001424052702303302504577327744009046230 ("A Wall Street Journal examination of 100 of the most popular Facebook apps found that some seek the email addresses, current location and sexual preference, among other details, not only of app users but also of their Facebook friends. One Yahoo service powered by Facebook requests access to a person's religious and political leanings as a condition for using it."); Elizabeth Dwoskin & Craig Timberg, *Google Knows When Its Users Go to the Store and Buy Stuff*, WASH. POST (May 23, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/05/23/google-now-knows-when-you-are-at-a-cash-register-and-how-much-you-are-spending/?utm_term=.277ad9e87871 (noting that Google "analyzes users' Web browsing, search history, and Geographic locations" through "Youtube, Gmail, Google Maps, and the Google Play store" and has recently started analyzing credit card records to prove the success of its ad campaigns).

[8] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY 3, 20, 28–31, 34, 36, 66, 78–79 (2015) (explaining how the term "black box" may mean a recording device, such as the data monitoring system in an airplane, or a system whose actual workings are difficult to discern, and noting that black box technologies have been used to determine health status, personality, eligibility for employment, and consumer habits); *see generally* MIKOŁAJ JAN PISKORSKI, A SOCIAL STRATEGY: HOW WE PROFIT FROM SOCIAL MEDIA (2014).

[9] *See* TIM WU, ATTENTION MERCHANTS (2017); NIR EYAL, HOOKED (2013).

[10] *See* SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING: (AND WHY WE SHOULD WORRY) 2, 6–7, 61 (2011) (stating that "*Google* is used as a noun and a verb" and observing that Google influences ideologies and how its users interact with the world); *Swipe Right (Or Left)*, OXFORD LIVING DICTIONARIES, https://en.oxforddictionaries.com/definition/swipe_right_(or_left) (last visited July 29, 2017) (defining the terms "swipe right," meaning attractive, and "swipe left," meaning unattractive, which originated from the online dating app Tinder). *See also* Mark Molloy, *Facebook Addiction 'Activates Same Part of the Brain as Cocaine'*, TELEGRAPH (Feb 17, 2016, 2:15 PM), http://www.telegraph.co.uk/news/12161461/Facebook-addiction-activates-same-part-of-the-brain-as-cocaine.html (explaining a scientific study that suggests that Facebook use "affect[s] our grey matter in a similar way that cocaine does").

[11] *See, e.g.*, Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. (forthcoming Aug. 2017) (manuscript at 4–5, 26), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929643 (stating that companies like Google, Facebook, and Uber benefit from monetizing the data collected from their users, making the user of their services the product, not the consumer).

But profits in this context also are the spoils of a legal regime that effectively absolves online intermediaries from minding the harmful third-party user content that they host and repurpose for commercial gain. They are the benefits of a legal protection that almost no other entity in other legislative fields enjoys.[12]

Indeed, under current law, providers benefit from an immunity that allows them to repurpose user data in ancillary or secondary markets based on the happy but outdated fiction that such companies are only facilitating user connections. Many online intermediaries, after all, convey agnosticism about the substance of their users' online conduct. In doing so, they dramatically understate the extent to which they pull the strings from behind the scenes. But it is one thing to purport to administer an ostensibly neutral application and another matter to exploit user data to engineer how users communicate, socialize, and transact business in other markets.

This is how the CDA immunity doctrine, born over two decades ago, is at odds with the world as it is today. Internet intermediaries are structuring online content, conduct, and the entire networked environment in ways that the current doctrine does not contemplate.[13] The consequences of this failing are troubling and require reform.[14]

Consider two prominent online applications that connect people in the housing market: Facebook and Airbnb. Facebook is most well-known for its flagship social network application, through which it collects and analyzes information about users' friend networks, communities of interest, and "likes" to personalize each user's experience and connections. This is the service for which most users sign up. But the company does so much more with user data. First, it sells it to advertising networks and data

---

[12] *But see* David Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures Of Information*, 127 HARV. L. REV. 512, 606 (2013) (discussing the "source/distributor divide" in the context of government leaks).

[13] *Cf.* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. (forthcoming 2018); Elizabeth Kolbert, *Who Owns the Internet?*, NEW YORKER (Aug. 28, 2017), https://www.newyorker.com/magazine/2017/08/28/who-owns-the-internet.

[14] The most well-known reform proposal would remove the immunity for publishing content that enables sex trafficking. *See, e.g.*, Stop Enabling Sex Traffickers Act of 2017, S. 1693, 115th Cong. (2017). Danielle Citron and Benjamin Wittes argue persuasively for reform in a law review article published shortly before this one. *See* Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORD. L. REV. 401 (2017). Google has underscored the powerful gatekeeping role in our networked information economy if news reports that it is "manipulating its search engine results to favor opposition to" the legislation are to be believed. *See* PR Newswire, *Google Appears to Be Manipulating Its Search Engine Results to Defend Internet Law that Enables Sex Trafficking, Consumer Watchdog Finds*, BUS. INSIDER (Sept. 11, 2017), http://markets.businessinsider.com/news/stocks/Google-Appears-to-Be-Manipulating-Its-Search-Engine-Results-to-Defend-Internet-Law-that-Enables-Sex-Trafficking-Consumer-Watchdog-Finds-1002359550.

brokers. Second, and more pertinently, it relies on the information it learns about users to offer advertisers the powerful ability to market products and services to potential "microtargeted" buyers.[15] Until very recently, the company allowed advertisers to target users based on their "ethnic affinities" through this distinct but ancillary service.[16] Thus, a hypothetical building manager or broker could advertise an apartment for rent and distribute the ad to people whose "ethnic affinities" fit a profile that he or she prefers. With this designation, the service enables our manager or broker to exclude people on that basis as well.

Facebook's advertisement service is not limited by industry. An advertiser can reach audiences across product types, from cosmetics to sports clothing to kitchen appliances. Airbnb's service, on the other hand, enables members to advertise short-term rentals or apply to stay at those listings. It urges members to share personal information, including their names and personal profile pictures, which it, in turn, reserves the right to sell to travel management partners and other third parties.[17] The company personalizes accounts to engender an authentic connection between hosts and guests in ways that conventional online classified sites like Craigslist do not. This ambition for fostering trusted and authentic connections comes at a cost—when hosts look to accept someone they trust into their homes, they look for familiar signs, including the potential guest's race. According to a Harvard Business School study, hosts systematically discriminate against racial minorities based on the latter's pictures and names.[18] As difficult as it is to detect when hosts are racist in their guest

---

[15] *See, e.g.*, Ciara Torres-Spelliscy, *Shooting Your Brand in the Foot: What* Citizens United *Invites*, 68 RUTGERS U. L. REV. 1297, 1324–25 (2016) ("[I]nformation filter[s] place[] consumers in isolated 'tribes'. . . . [T]o the extent customers are living in their own tribal worlds, marketers will try to reach the customer in their respective bubbles. This means mass marketers increasingly need to micro-target sub-demographic groups." (footnotes omitted)). Facebook also sells data to be used in political campaigns. Allison Brennan, *Microtargeting: How Campaigns Know You Better Than You Know Yourself*, CNN (Nov. 5, 2012, 6:45 PM), http://www.cnn.com/2012/11/05/politics/voters-microtargeting/index.html (explaining how Facebook sells information to political campaigns so that the campaigns may microtarget certain favorable demographics with political ads).

[16] Julia Angwin & Terry Parris, Jr., *Facebook Lets Advertisers Exclude Users by Race*, PROPUBLICA (Oct. 28, 2016, 8:00 AM), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race; Annalee Newitz, *Facebook's Ad Platform Now Guesses at Your Race Based on Your Behavior*, ARS TECHNICA (Mar. 18, 2016, 5:15 PM), https://arstechnica.com/information-technology/2016/03/facebooks-ad-platform-now-guesses-at-your-race-based-on-your-behavior/.

[17] *Privacy Policy*, AIRBNB, https://www.airbnb.com/terms/privacy_policy (last visited July 31, 2017).

[18] *See* Benjamin Edelman, Michael Luca, & Dan Svirsky, *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, 9 AM. ECON. J.: APPLIED ECON. 1, 2 (2017) ("We find widespread discrimination against guests with distinctively African American names. African American guests received a positive response roughly 42 percent of the time, compared to roughly 50 percent for white guests.").

selection, anecdotal reports of Airbnb-facilitated discrimination surface with enough frequency to suggest that the practice is not rare.[19]

There are good reasons to be concerned about these aspects of the Facebook advertising service and Airbnb. Consider in particular the way in which both services enable advertisers to target their ads based on information that is barred by anti-discrimination laws. The 1968 Fair Housing Act (FHA) specifically forbids home sellers or renters, as well as brokers, property managers, and agents, from distributing advertisements "that indicate[] any preference, limitation, or discrimination based on race, color, religion, sex, handicap, familial status, or national origin . . . ."[20] Both companies have defensible arguments that they may not be held liable for the discriminatory online behavior of their users under the prevailing immunity doctrine. Under this theory, they simply provide the tools on which users, landlords, and building managers rely as they please. In the language of the current doctrine, neither Facebook nor Airbnb are materially contributing to the objectionable content.

Yet, these companies know that they may be doing something wrong, if not illegal. Both companies have taken steps to diminish the racially discriminatory impact of their respective applications in recognition of the role that their applications may play. Airbnb commissioned a prominent civil rights attorney to study hosts' use of the application.[21] This report was not an empirical study of Airbnb host racism as such. But its findings acknowledged patterns of discrimination and recommended remedial steps, all of which the company adopted.[22] Airbnb also announced that it would redouble its commitment to nondiscrimination.[23] While it has not discontinued the use of photographs, the main concern of civil rights groups, it now has a strict policy of removing members who use the application in ways that violate civil rights laws.[24]

Facebook, for its part, reformed its audience selection policy in the advertising service, replacing the "ethnic affinity" classifications with what

---

[19] *See, e.g.*, Kristen Clarke, *Does Airbnb Enable Racism?*, N.Y. TIMES (Aug. 23, 2016), https://www.nytimes.com/2016/08/23/opinion/how-airbnb-can-fight-racial-discrimination.html (describing the African American author's unusual difficulty in booking an Airbnb reservation); Carla Javier, *A Trump-Loving Airbnb Host Canceled This Woman's Reservation Because She's Asian*, SPLINTER NEWS (Apr. 6, 2017, 4:11 PM), http://splinternews.com/a-trump-loving-airbnb-host-canceled-this-womans-reserva-1794086239 (reporting that an Asian woman's Airbnb reservation was cancelled abruptly and displaying screenshots of text messages where the host said: "I wouldn't rent to u [sic] if u [sic] were the last person on earth. One word says it all. Asian.").

[20] 42 U.S.C. § 3604(c) (2007).

[21] LAURA MURPHY, LAURA MURPHY & ASSOCS., AIRBNB'S WORK TO FIGHT DISCRIMINATION AND BUILD INCLUSION: A REPORT SUBMITTED TO AIRBNB 10 (2016), http://blog.airbnb.com/wp-content/uploads/2016/09/REPORT_Airbnbs-Work-to-Fight-Discrimination-and-Build-Inclusion.pdf.

[22] *Id.* at 10–12.

[23] *Id.* at 12.

[24] *Id.* at 10–11.

it now calls "multicultural affinity."[25] The company also now prohibits users from targeting or excluding specific groups of people from seeing ads for housing, credit, or employment.[26] It requires advertisers to certify that their practices comply with its nondiscrimination policies and antidiscrimination laws.[27]

These are important steps. But, one year later, Facebook reportedly continues to enable advertisers to discriminate against protected classes.[28] In any event, Facebook's (ostensibly failing) efforts to reform are not enough to stop discrimination in other online markets for housing. What of all other applications and marketplaces that purport to be content agnostic about online conduct, but whose designs enable users to do bad things they might not otherwise be able to do? Under the current doctrine, liability may not reach intermediaries that routinely host illegal content by design. And, in any event, bigoted advertisers will continue to use Facebook's service notwithstanding the proviso from Facebook that such uses are not permitted. Other services, moreover, may choose not to respond in the same way that Facebook has.

The immunity under the CDA, codified at 47 U.S.C. § 230, gives such intermediaries cover largely because courts have read the protection broadly. And they have had good reason to. The first operative provision of the statute states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[29] Congress's reference here to "publisher or speaker" draws from defamation law doctrine, where a defendant publisher is as liable for republishing reputation-damaging

---

[25] *Improving Enforcement and Promoting Diversity: Updates to Ads Policies and Tools*, FACEBOOK NEWSROOM (Feb. 8, 2017), http://newsroom.fb.com/news/2017/02/improving-enforcement-and-promoting-diversity-updates-to-ads-policies-and-tools/. *See also* Sapna Maheshwari & Mike Isaac, *Facebook Will Stop Some Ads From Targeting Users by Race*, N.Y. TIMES (Nov. 11, 2016), https://www.nytimes.com/2016/11/12/business/media/facebook-will-stop-some-ads-from-targeting-users-by-race.html?_r=0 ("Facebook responded on Friday to concern that it was violating anti-discrimination laws, announcing that marketers placing housing, employment or credit ads on the social network would no longer be able to use tools that target people by ethnicity.").

[26] *See Improving Enforcement and Promoting Diversity: Updates to Ads Policies and Tools*, *supra* note 25 ("[A]dvertisers may not discriminate against people based on personal attributes such as race, ethnicity, color, national origin . . . . When an advertiser attempts to show an ad that we identify as offering a housing, employment or credit opportunity and either includes or excludes our multicultural advertising segments—which consist of people interested in seeing content related to the African American, Asian American and US Hispanic communities—we will disapprove the ad.").

[27] *See id.* ("When an advertiser attempts to show an ad that we identify as offering a housing, employment or credit opportunity and uses any other audience segment on Facebook . . . . [w]e will . . . require the advertiser to certify that it is complying with that policy and with applicable anti-discrimination laws.").

[28] See Julia Angwin, Ariana Tobin, and Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, PROPUBLICA (Nov. 21, 2017), https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin?utm_campaign=sprout&utm_medium=social&utm_source=twitter&utm_content=1511288776.

[29] 47 U.S.C. § 230(c)(1).

material as its author.[30] When enacted in 1996, Section 230(c) was intended to bar courts from holding providers liable for publishing information that could harm users' reputation.

This was and remains an idiosyncratic and exceptional treatment under law. Newspapers and book imprints, for example, remain as liable for publishing unlawful classified advertisements or opinion editorials as the original authors are.[31] Legislators in 1996 expressed the view that providers of online services and applications were different—that they should not be held to account for the massive amounts of third-party user content that they host and publish.[32] Parroting the emergent ethos among technologists and internet free-speech activists, legislators in this period found that imposing liability on online intermediaries for failing to screen or remove all offending content would exact a "chilling" toll on all users that is far greater than it would be for traditional publishers.[33] In such a world, providers would censor any content that they rightly or wrongly believe exposes them to liability.[34] Section 230 relieves intermediaries of that heavy burden in the interest of promoting entrepreneurship and freedom of expression online.

Most legislators in 1996, however, could not have anticipated that the internet would permeate public life or that intermediaries would engineer practically all our online conduct. They did appreciate, however, that the protection could not be absolute. Section 230 specifically provides that the immunity recedes when the provider in question "is responsible, in whole or in part, for the creation or development" of the offending information.[35]

---

[30] *See* RESTATEMENT (SECOND) OF TORTS § 578 (AM. LAW. INST. 1977) ("Except as to those who only deliver or transmit defamation published by a third person, one who repeats or otherwise republishes defamatory matter is subject to liability as if he had originally published it.").

[31] *See id.* at cmt. b ("It is no defense that the second publisher names the author or original publisher of the libel. Thus a newspaper is subject to liability if it republishes a defamatory statement . . . .").

[32] *See, e.g.*, 104 CONG. REC. 8471 (1995) (statement of Rep. Goodlatte) ("There is no way that any of those entities . . . can take the responsibility to edit out information that is going to be coming in to them from all manner of sources . . . . We are talking about something that is going to be thousands of pages of information every day, and to have that imposition imposed on them is wrong.").

[33] *See id.* (statement of Rep. Cox) ("If we regulate the Internet at the FCC, that will freeze or at least slow down technology. It will threaten the future of the Internet."); *id.* (statement of Rep. Lofgren) ("Really it is like saying that the mailman is going to be liable when he delivers a plain brown envelope for what is inside it. It will not work. It is a misunderstanding of the technology . . . . I would urge [47 U.S.C. § 230's] approval so that we preserve the first amendment and open systems on the Net.").

[34] *See* Wu, *supra* note 2, at 300 (noting that internet intermediaries, if exposed to liability, may delete a substantial amount of content, even content that is "lawful and socially desirable").

[35] 47 U.S.C. § 230(f)(3) (1998).

Congress also wrote in a "Good Samaritan" safe harbor to incentivize providers to mind their users' "objectionable" content.[36]

The courts have nevertheless adopted a very broad reading of the statute that belies these limits on immunity. The courts reason that, without this generous protection, the threat of litigation would chill providers' willingness to host and publish all but the most anodyne content.[37] So, even while a meaningful but small threat of litigation always remains, service providers today rest easy in knowing that they are not legally implicated by any of their users' harmful communications.

Today, the Good Samaritan, who is supposed to tend to the most vulnerable,[38] plays no role in the courts' administration of Section 230. In a glaring irony, the prevailing doctrine turns the biblical parable for which Congress named the operative provisions on its head.

To be fair, some of the objectives to which legislators aspired have come to pass. Users today have an abundance of ways to transact business and socialize online largely because entrepreneurs have felt safe to experiment and innovate, unconcerned by the potential for third-party wrongdoing. Yet, there is good reason to doubt that entrepreneurs needed the immunity to enter the market. Even in the mid-1990s, people understood that the internet's transmission protocols, interoperable network design, and end-user focus would transform markets and birth lucrative new ones. The internet was always promising, with or without the protection of Section 230. But the prevailing online immunity doctrine has removed much of the risk for entrepreneurs. This is largely why, today, applications and websites of all kinds, from the frivolous to the truly disruptive, seem to spring up nearly daily.

The current doctrine gives the online entrepreneurs behind these services no incentive to be Good Samaritans—or to even consider the social costs of their services. In this way, the courts have developed a broad immunity that could very well protect Facebook and Airbnb from liability for systematic third-party violations of the FHA. The doctrine, after all, is premised largely on the view that service providers should not have to police the massive amount of third-party content that flows through their servers. Bigoted advertisers in this conception are to blame, not the

---

[36] *Id.* § 230(c)(2)(A) ("No provider or user of an interactive computer service shall be held liable on account of . . . 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.")

[37] *See, e.g.*, Zeran v. America Online, 129 F.3d 327, 331 (4th Cir. 1997) ("Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted.")

[38] *See Luke* 10:25–37 ("[A] Samaritan, as he traveled, came where the man was; and when he saw him, he took pity on him. He went to him and bandaged his wounds, pouring on oil and wine. Then he put the man on his own donkey, brought him to an inn and took care of him.").

engineers of the "neutral" tools that facilitate connections. It is for this reason that neither Facebook nor Airbnb might be required to police the illegally discriminatory expressive acts of the millions of users of its services. Facebook does not discriminate in the housing market; its users and advertisers do. Airbnb does not require users to signify racial preferences; hosts do.

This Article proposes a reform that is adapted to the influence that developers of applications and marketplaces like Facebook and Airbnb have today. But I do not invent this recommendation out of whole cloth. While Section 230 doctrine to this point suggests that those specific companies would be immune for users' unlawful online conduct, developments of the past few years suggest that providers like Facebook and Airbnb should be wary. Courts have begun to pull away from their broad reading of Section 230 and attend more carefully to the ways in which online intermediaries *design* users' online content and transactions. While courts have instituted the high bar of "material contribution" to evaluate whether a provider had a hand in developing illegal content, they also have identified designs and conditions that define the substance of the information that users share.[39]

Based on these developments, I propose here that courts shield providers from liability for third-party online conduct only to the extent they either are true passive conduits or actually take good-faith steps to remove or block illegal content. In some regards, this is a reframing of the Good Samaritan safe harbor that Congress already articulated in the statute. But, importantly, it pivots away from conditioning immunity only on "restrict[ing] access" to "objectionable" content.[40] The proposal here instead would bar immunity when providers process and publish user data in ancillary or secondary markets in ways such that their users do not knowingly or directly benefit. In practice, this approach would likely continue to shield intermediaries that do nothing more than provide the adverted networking and marketplace service, but would likely not shield those like Facebook or Airbnb that sell user data to advertisers to varying extents.

---

[39] *See* FTC v. Accusearch, Inc., 570 F.3d 1187, 1198–99 (10th Cir. 2009) (holding that "develop[ment]," in the context of the CDA, means to "draw[] something out, making it visible, active, or usable," and that intermediaries are "responsible" for the development of offensive content if they "specifically encourage[] development of what is offensive about the content" (internal quotation marks omitted)); Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1165, 1167 (9th Cir. 2008) (stating that "[t]he CDA does not grant immunity for inducing third parties to express illegal preferences" and holding that Roommate.com, an internet intermediary, developed offensive content by directing its users to sort potential housing mates by personal characteristics such as race, gender, and sexuality).

[40] 47 U.S.C. § 230(c)(2)(A) (1998).

While I claim novelty here, I do so mindful of the massive number of law review pages devoted to the topic of online intermediary immunity. To the extent this Article offers anything new, it is in its argument that online intermediary designs implicate online services and applications far more than courts have recognized to this point.[41] In this regard, it adds another dimension to the argument that Congress ought to narrow the scope of protection under the statute for publication of harmful material like nonconsensual porn.[42] This Article also identifies the ways in which content agnosticism has the effect of harming historically subordinated groups in historically fraught legal markets like housing, employment, and credit. Communications law in the United States encourages inclusion as a matter of course.[43] The safe harbor under Section 230, I argue, should similarly be read to apply to firms that take affirmative steps in good faith to protect against unlawful—that is, systematically discriminatory—online behavior.

This Article makes its argument in four parts. Part I describes the current ways in which intermediaries collect and generally interact with information from users. The range of prominent design features, from anonymity to ephemeral messaging, suggests that providers have far more agency in choosing how to structure their services and applications. They are generally motivated, moreover, by commercial incentives that often counsel for structuring applications and services that are far more determinative of user content than the prevailing doctrine presumes. Part II describes the evolution of the current doctrine, from the high-minded and broad protection of intermediaries in the late 1990s to its current refinements and elaborations. In this evolution, I show that service and application designs have come into sharper focus for courts. Part III builds on this account to demonstrate the ways in which the current doctrine has created an opening for considering the ways in which intermediary designs determine user content and online conduct. Finally, in Part IV, the Article returns to the example of Facebook's

---

[41] There are important overlaps, moreover, with the contemporaneously published piece by Danielle Citron and Benjamin Wittes on the limitations of current doctrine and the need for reform addressed to gender-based abuse and sex trafficking. *See* Citron & Wittes, *supra* note 14.

[42] *See* Stop Enabling Sex-Traffickers Act of 2017, S. 1693, 115th Cong. (2017); Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORD. L. REV. 401 (2017).

[43] *See* 47 U.S.C. § 151 (1996) (stating that the Federal Communications Commission was created "[f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex, a rapid, efficient, Nation-wide, and world-wide wire and radio communication service"); Olivier Sylvain, *Network Equality*, 67 HASTINGS L.J. 443, 449 (2016) ("The FCC has declared that the Internet is a public general use technology—like electricity—and, accordingly, must be treated under law as a common carrier. Under this rule, service providers must ensure that all members of the public who try to access the Internet are treated equally.").

advertising service to argue that, indeed, there are compelling reasons for reading Section 230 far more carefully in today's online environment.

## I. ANTISOCIAL MEDIA

Policymakers, technologists, and activists have had great hopes for the internet. The excitement about its promise was no more feverish than in the first decade or so after Congress fully commercialized it in 1995. The general view then was that the internet's transmission protocols, distributed and interoperable network design, and end-user focus would cause deep structural transformations everywhere and in all aspects of life.[44] Nongovernmental consensus-driven administration and standards would govern.[45]

It is this ethos that gave rise to 47 U.S.C. § 230—one of the most important legislative enactments addressed to internet services and applications.[46] Among other things, Section 230 (entitled the Communications Decency Act) shields providers of "interactive computer service[s]" from liability for content that their third-party users circulate through the online service.[47] As written, this protection, however, does not reach applications that are in any part "responsible . . . for the creation or development" of "objectionable" material.[48] But there is more to the statute than a simple reform of defamation law. Through it, Congress explicitly shields service providers from liability for exercising "Good Samaritan" editorial judgment about substantive content. That is, the immunity applies to services that edit, filter, or take down objectionable material, or help users to do so.[49]

Courts read Section 230 extremely broadly in spite of how it is written. They hold that the provision immunizes networked services and online

---

[44] David R. Johnson & David G. Post, *Law And Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUNDATION (Feb. 8, 1996), https://www.eff.org/cyberspace-independence; Esther Dyson et al., *Cyberspace And The American Dream: A Magna Carta For The Knowledge Age*, FUTURE INSIGHT (Aug. 1994), http://www.pff.org/issues-pubs/futureinsights/fi1.2magnacarta.html.

[45] Johnson & Post, *supra* note 44, at 1367; Barlow, *supra* note 44; Dyson et al., *supra* note 44.

[46] The Communications Decency Act is Title V of the Telecommunications Act of 1996. Communications Decency Act of 1996, Pub. L. No. 104–104, § 230, 110 Stat. 56, 137–39 (1996) (codified as amended at 47 U.S.C. § 230 (1998)).

[47] 47 U.S.C. § 230(c)(1) (1998). The statute explicitly preempts state tort law. Section 230(e)(3) provides, among other things, that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." *Id.* § 230(e)(3).

[48] *Id.* §§ 230(c)(2)(A), (f)(3).

[49] *Id.* Section 230(c)(2) shields interactive computer services that have voluntarily taken steps in good faith to censor or take down "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 . . . ." *Id.* I return to the particulars of the statute—its text, history, and purposes—*infra* Part II.

applications from liability for publishing the illegal content of their users.[50] So, under current law, a social media company cannot be held responsible for allowing a user to post compromising private photographs of his ex-girlfriend publicly.[51] A search engine cannot be called to task under law for displaying the advertisements of third parties that sell copyrighted ringtones.[52] An online advertising service is under no legal obligation to remove posts that encourage the sex trafficking of minors.[53]

Two decades later, there is reason to believe that Section 230 and the information libertarianism on which it is based have been a great success.[54] The internet's remarkably rapid integration into public life over the past two decades has arguably shown that application developers, free from the threat of government regulation or tort liability, can be good stewards of life and commerce online. Popular applications like YouTube, the video-sharing site, and Reddit, the news aggregation and discussion site, have developed conventions and software for the moderation of user content, even as users create, contribute, and interact prodigiously.[55] These services are the conduits envisioned by the early proponents of broad

---

[50] *See supra* notes 4–5 and accompanying text.

[51] *See* Barnes v. Yahoo!, Inc., 570 F. 3d 1096, 1098, 1102–04 (9th Cir. 2009), *amended by* Barnes v. Yahoo, Inc., 2009 U.S. App. LEXIS 21308 (9th Cir. 2009) (holding that Yahoo! was not responsible for one of its users posting an ex-girlfriend's nude photographs on his profile).

[52] *See* Goddard v. Google, Inc., 640 F. Supp. 2d 1193, 1195, 1197–98, 1202 (N.D. Cal. 2009) (holding that Google was not responsible for fraudulent advertisements that were posted on Google's websites).

[53] Doe v. Backpage.com, LLC, 817 F.3d 12, 16, 18–22 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017).

[54] *See generally* Jane R. Bambauer & Derek E. Bambauer, *Information Libertarianism*, 105 CAL. L. REV. 335 (2017).

[55] YouTube removes or age restricts "nudity or sexual content," "harmful or dangerous content," copyrighted content, "hateful content" which "promotes or condones violence against individuals or groups," "threats," and "spam, misleading metadata, and scams." *Community Guidelines*, YOUTUBE, https://www.youtube.com/yt/policyandsafety/communityguidelines.html (last visited Aug. 5, 2017); *Nudity and Sexual Content*, YOUTUBE, https://support.google.com/youtube/answer/2802002 (last visited Aug. 5, 2017). YouTube removes inappropriate content through a "flagging" system, where YouTube users "flag" videos or comments and a member of YouTube staff reviews the video or comment and removes it if it violates the community guidelines. *Id.* YouTube also uses a system called "Content ID," which compares user uploads to copyrighted content and automatically blocks, monetizes, or tracks the content if it finds a match. *How Content ID Works*, YOUTUBE, https://support.google.com/youtube/answer/2797370?hl=en (last visited Aug. 5, 2017). Reddit relies heavily on volunteer moderators, who are capable of removing content, banning users from their "subreddits," and creating "AutoModerator," which are "bot" that remove certain kinds of content automatically. *Moderation*, REDDIT, https://www.reddit.com/wiki/moderation (last visited Aug. 5, 2017). Reddit, which emphatically champions free speech, was criticized in 2015 for permanently banning five "questionable" subreddits. *See, e.g.*, Caitlin Dewey, *These Are the Five Subreddits Reddit Banned Under Its Game-Changing Anti-Harassment Policy—And Why it Banned Them*, WASH. POST (June 10, 2015), https://www.washingtonpost.com/news/the-intersect/wp/2015/06/10/these-are-the-5-subreddits-reddit-banned-under-its-game-changing-anti-harassment-policy-and-why-it-banned-them/?utm_term=.92bf470cd3b4 (discussing Reddit's actions in banning subreddits "dedicated to fat-shaming," "transphobia," " racism," and "to harassing members of a progressive video game site").

immunity for providers, helping to transform the internet into the "forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[56] And they have done so with a "minimum of government regulation."[57]

But, today, online intermediaries are more than open forums for user-generated discourse, cultural development, and intellectual activity. Those priorities have given way to or, rather, have been complicated by pecuniary ones. In the mid-2000s, prominent observers of the networked-information economy debated whether for-profit motivations would predominate online.[58] There is little question, however, that most application developers today have either succumbed to the commercial prerogatives of the large corporations that have bought them or, having become large companies themselves, have leveraged their market position to develop ancillary or secondary lines of business.

Today, online services do so much more than relay or store user-generated content in the way that the early proponents of immunity and nongovernmental interference presumed. They actively shape every aspect of the user experience.[59] Many of the most successful internet companies, moreover, design their applications to collect, analyze, sort, reconfigure, and repurpose user data for their own commercial reasons, unrelated to the original interest in publishing material or connecting users.[60] These developments belie any suggestion that online intermediaries are merely conduits of user information anymore. Today, to the extent a company purports to be agnostic about its users' content, it generally does so mindful that its design will invite a wide range of content, including illegal or otherwise antisocial material.

Content moderation like that employed by YouTube or Reddit, therefore, is only a piece of how intermediaries manage user content. And this is an important point, as it suggests that the original logic for immunity is incomplete or simply wrong. Indeed, providers today are far more implicated in the kinds of content that users create or commercial transactions into which users enter. So, in order for the immunity doctrine to be addressed to our current state of affairs, the courts will have to revise

---

[56] 47 U.S.C. § 230(a)(3).

[57] *Id.* § 230(a)(4).

[58] *See, e.g.*, Mathew Ingram, *The Carr-Benkler Wager and the Peer-Powered Economy*, GIGAOM (May 9, 2012, 3:02 PM), https://gigaom.com/2012/05/09/the-carr-benkler-wager-and-the-peer-powered-economy/ (discussing a 2006 bet between author Nick Carr and Harvard professor Yochai Benkler, where Benkler wagered that the internet is primarily based on "commons-based peer production" and Carr wagered that content sharing networks were only successful because a market had not yet developed for online goods).

[59] *Cf.* Klonick, *supra* note 13; Kolbert, *supra* note 13.

[60] *See supra* notes 7, 8, 15 and accompanying text. This is to say nothing of the myriad of ways in which companies use algorithmic processing and machine learning to predict user online behavior.

their current approach. As I recommend later, the doctrine would have to require courts to consider whether intermediaries' designs create the conditions under which their users unavoidably engage in illegal activity.

Before turning to reform, however, this Part describes our current state of affairs. First, I outline the ways in which applications that rely on user-generated content manage their users' interactions, even while they purport to be mere passive hosts. To do this, I review the way in which some of the most recognizable online intermediaries today have chosen to moderate user content and interactions. And while moderation has emerged as an important way of managing user interactions, I then show that popular intermediaries today, namely, Airbnb and Facebook, are constantly managing the design of their applications in order to structure the manner in which user content gets shared and manipulated by others. The lesson in all of this is that, today, as application designs become ever more determinative of online conduct, we might expect that the scope of immunity would recede.

### A. *Moderating User Content*

Through Section 230, Congress sought to encourage online intermediaries to be passive conduits that facilitate end users' communications and transactions. Providers in this conception contribute nothing original or material to their users' content. They only undertake a limited set of operations to support user creativity and user-to-user interaction, agnostic about the substance of the thing. Under the current doctrine, this relative unconcern with content qualifies a provider for immunity. Congress sought to protect these kinds of services and applications in order to encourage content diversity and the free flow of information on the internet.[61] Courts, in interpreting Section 230, presumed that, without the protection, providers would be chilled into censoring unpopular or unsavory online user conduct far more than necessary to avoid even the possibility of liability.[62]

Today, several popular web-based applications continue to embody this laissez-faire conception, operating as simple "platforms" for the distribution of user-generated content.[63] YouTube, the video-sharing

---

[61] *See* 47 U.S.C. § 230(a)(3) (2012) ("The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.").

[62] *See* Wu, *supra* note 2, at 300, 315–18 (stating that Congress's intent in passing Section 230 was vague, but that courts interpreted the statute to mean that internet intermediaries should not be subject to liability, as it would have a "chilling effect" on freedom speech on the internet).

[63] The platform metaphor itself is very evocative and, as such, often used by scholars in information and communications law. *See, e.g.*, Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV. 87, 94 (2016) (stating that "a platform company is launched as an online intermediary between buyers and sellers of goods and services—the ancient role of the middle man"); Richard S. Whitt,

application, is probably the most recognizable of these. On the one hand, it has become invaluable to the promotion and distribution of videos by professionals and major production studios. But, as the company's name and slogan "Broadcast Yourself" suggest, YouTube markets itself above all as a democratic forum through which any and all users may express themselves.[64] Its administrators only manage registration, suspension, or deletion of user accounts, the means by which users upload videos, and features through which other users may rank or comment on the post.[65] While the company enters into distribution and syndication arrangements with content developers, at the core of the YouTube business, as with most applications that rely on user-generated content, is a faith in the creativity and agency of users as creators and discriminating consumers.

This is to say nothing of the way in which the service has helped to disintermediate hub-and-spoke video distribution models in, for example, broadcasting and cable television. By creating a platform for individual users to post videos, YouTube has helped to foster a whole new logic and political economy for content distribution. In this way, it is the quintessential exemplar of what Congress and scholars must have had in mind twenty years ago.

But questions remain about the extent to which YouTube or other user-generated video sharing applications must actively monitor and, in some ways, shape content on their sites.[66] The company has been the defendant in secondary liability claims in a variety of cases, including a widely publicized billion-dollar lawsuit for hosting high-value copyrighted material posted by third-party users without authorization.[67] It is clear

---

*Evolving Broadband Policy: Taking Adaptive Stances to Foster Optimal Internet Platforms*, 17 COMMLAW CONSPECTUS 417, 439 (2009) (using platform as a "helpful metaphor" to argue that the purpose of broadband is "to serve as a platform for allowing end users to utilize the capabilities of the Internet"). The metaphor, however, has its limitations, as it assumes too much. Frank Pasquale offers a more nuanced and productive point of view. *See generally* Frank Pasquale, *Two Narratives of Platform Capitalism*, 35 YALE L. & POL'Y REV. 309 (2016).

[64] *See, e.g.*, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 28 (2d Cir. 2012) ("Under the slogan 'Broadcast yourself,' Youtube achieved rapid prominence and profitability . . . .").

[65] *See, e.g.*, *id.* (stating that YouTube requires users to register for an account and requires users to agree to its terms of service, but does not create, strictly moderate, or review all content uploaded to the site).

[66] For example, if the intermediaries have "actual knowledge" of hosting copyrighted material, they may be open to liability if they do not take sufficient steps to remove the illegal content. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1024–25 (9th Cir. 2013). *See Viacom Int'l, Inc.*, 676 F.3d at 33–34 (discussing email conversations wherein the YouTube founders, Jared Karim and Chad Hurley, debated the costs and benefits of removing specific copyrighted materials from the site, which exposed YouTube to liability for hosting the illegal content).

[67] *See Viacom Int'l, Inc.*, 676 F.3d at 28–29 (summarizing a class action suit brought against YouTube, where a group of several copyright holders brought suit against YouTube for knowingly hosting 63,497 videos containing copyrighted material). Viacom originally sued YouTube for $1 billion; the case was settled and the terms of the settlement were not disclosed. *See* Jonathan Stempel,

from these cases that YouTube and other video sharing sites like it can and indeed do moderate which user-generated content appears on the service, even if it does not create or edit the content once up. Indeed, YouTube in particular administers a "Partner Program" through which users can syndicate video programming through the service,[68] as well as Content ID, which empowers copyright holders to track unauthorized posts by users of their content.[69]

Yet, irrespective of the extent to which YouTube monitors or engages users' content, the service remains mostly a disinterested repository for uninhibited user expression, hosting an astounding number of videos addressed to almost all humanly-known topics. In this way, YouTube resembles a conduit through which all user content may reach every user of the application. But, again, it is not a purely passive conduit, as it structures the ways in which users post and monitor content.

As with most providers like it, YouTube recognized the perils of designing its service in this way early on. It, again, like most user-generated content platforms, requires its users to abide by "Community Guidelines." Failure to adhere will lead to account suspension or termination.[70]

Even Reddit, an online website that has been evangelical about its non-interventionist approach to user-generated content since its founding in 2005, has reformed its approach over the last couple of years. Like YouTube, Reddit allows registered users to comment on and vote up or down stories and posts from any source.[71] The community of users assigns each story to a predetermined category—say, in movies, gaming, and "futurology."[72] But Reddit allows registered users to initiate discussion

---

*Google, Viacom Settle Landmark YouTube Lawsuit*, THOMSON REUTERS (Mar. 18, 2014, 9:05 AM), http://www.reuters.com/article/us-google-viacom-lawsuit-idUSBREA2H11220140318. In 2015, an actress brought a suit against YouTube for hosting an edited, controversial video of herself, for which she received death threats. Garcia v. Google, 786 F.3d 733, 736–38 (9th Cir. 2015). The actress alleged that she owned the copyright for her own image, but her claim ultimately failed on that ground. *Id.* at 740–41, 744, 747.

[68] *YouTube Partner Program Overview*, YOUTUBE, https://support.google.com/youtube/answer/72851?hl=en (last visited Oct. 27, 2017).

[69] *How Content ID Works*, YOUTUBE, https://support.google.com/youtube/answer/2797370?hl=en (last visited Nov. 4, 2017)

[70] *Community Guidelines*, YOUTUBE, https://www.youtube.com/yt/policyandsafety/en-GB/communityguidelines.html (last visited Aug. 5, 2017) ("Accounts are penalised [sic] for Community Guidelines violations, and serious or repeated violations can lead to account termination.").

[71] *See, e.g.*, Andrew Couts, *How to Get a Link on the Front Page of Reddit*, DIGITAL TRENDS (Apr. 12, 2013, 12:02 PM), https://www.digitaltrends.com/how-to/how-to-get-a-link-on-the-front-page-of-reddit/ ("Once a link is submitted, other users can either "upvote" or "downvote" the link. They can also comment on the link.").

[72] *Futurology*, REDDIT, https://www.reddit.com/r/Futurology/ (last visited Aug. 5, 2017); *Gaming*, REDDIT, https://www.reddit.com/r/gaming/ (last visited Aug. 5, 2017); *Movies*, REDDIT, https://www.reddit.com/r/movies/ (last visited Aug. 5, 2017).

threads called "subreddits."[73] The popularity of any post determines its location on the site, with the most popular being the most visible on the first entry page.[74] This bottom-up, democratic design has made Reddit a celebrated site among online speech enthusiasts.

Reddit, however, also has fallen victim to its own design as it finds itself hosting provocative posts and subreddits, including those that promote terrorist or misogynist violence.[75] In response to substantial pushback from users over the past couple of years, the company has revised its extremely laissez-faire position. In early 2017, for example, it adopted a "Content Policy" that, on the one hand, promotes the site as the "home to some of the most authentic content anywhere online," but, importantly, also recognizes the value of "show[ing] enough respect to others so that we all may continue to enjoy Reddit for what it is."[76] Among other things, the policy explicitly prohibits "illegal" content, "involuntary pornography," material that "[e]ncourages or incites violence," and content that "[t]hreatens, harasses, or bullies or encourages others to do so."[77]

This reform has been met with palpable resistance from some very vocal users. In response to efforts by the company to ban misogynist threads under this new policy,[78] for example, "redditors" and online

---

[73] *See What Are Communities or "Subreddits"?*, REDDITHELP, https://reddit.zendesk.com/hc/en-us/articles/204533569-What-are-communities-or-subreddits (last visited Aug. 5, 2017) (defining "subreddits" as "sub-communities within reddit . . . created and moderated by users . . . dedicated each to certain topics or ideas").

[74] *See, e.g.*, Couts, *supra* note 71 ("Once a link is submitted, other users can either 'upvote' or 'downvote' the link . . . . Submitted posts rise or fall based on the number of upvotes, which add to the overall 'karma' score of the post, versus the number of downvotes, which are subtracted from the overall score. . . . The posts with the greatest number of upvotes in a each subreddit can rise to the coveted front page.").

[75] *See* Rob Crilly, *Reddit Takes Down Forum Used To Share Stolen Celebrity Photographs*, TELEGRAPH (Sep. 8, 2014, 10:16 AM), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11080844/Reddit-takes-down-forum-used-to-share-stolen-celebrity-photographs.html ("The news and social networking site Reddit has removed a platform that last week allowed users to share a cache of stolen celebrity images, many of them explicit. They included naked pictures of Jennifer Lawrence, the Oscar-winning actress, and allegedly more than 100 other A-listers obtained by a hacker . . . ."); Charlie Warzel, *Reddit Is a Shrine to the Internet We Wanted and That's a Problem*, BUZZFEED (June 19, 2015, 3:05 PM), https://www.buzzfeed.com/charliewarzel/reddit-is-a-shrine-to-the-internet-we-wanted-and-thats-a-pro?utm_term=.bwnAJV57v#.wm472kR31 (discussing Reddit's ban of five offensive subreddits, including /r/transfags and /r/fatpeoplehate, and noting how many users objected to new restrictions on free speech).

[76] *Reddit Content Policy*, REDDIT, https://www.reddit.com/help/contentpolicy/ (last visited Aug. 5, 2017).

[77] *Id. See also Removing Harassing Subreddits*, REDDIT (June 10, 2015), https://np.reddit.com/r/announcements/comments/39bpam/removing_harassing_subreddits/ (announcing Reddit's intention to remove subreddits that are used as tools to harass people).

[78] *See Reddit Content Policy*, *supra* note 76 (restricting content commonly associated with misogyny, such as "involuntary pornography").

free-speech enthusiasts voted up comments that addressed Reddit's Asian-American female CEO in racist and misogynist ways.[79] These users were successful enough to push the hateful comments to the site's front page.[80] Since this episode, the company has hired more personnel to manage or moderate subreddits and comments. Reddit today is walking a fine line between promoting user content and touting itself as the "first page of the Internet."[81]

## B. *Designing User Content*

The difficulty of administering an open platform that all people feel free to join in spite of the "openness" is not unique to popular intermediaries like YouTube and Reddit. All major online services and applications that host user-generated content have one way or another had to negotiate the line between free expression on the one hand and inclusion on the other.[82]

In this way, provider moderation inverts the laissez-faire concerns about content regulation because it protects users against the chill occasioned by abusive or harassing online conduct. Moderation in this

---

[79] Warzel, *supra* note 75 ("In response to the ban, scorned redditors flooded the site, using the site's voting mechanisms to post crude racist and sexist comments disparaging Pao. Renderings of the CEO as a communist leader quickly hit the site's front page. Subreddits like /r/PaoYongYang and /r/EllenPao_IsA_Cunt popped up as well as petitions calling for her resignation.").

[80] *Id.*

[81] In response to similar content policy reforms by other such providers, some users have begun to lament the end of the World Wide Web or even the internet as a space for free online expression. *See, e.g.*, Kalev Leetaru, *How Twitter's New Censorship Tools Are the Pandora's Box Moving Us Towards the End of Free Speech*, FORBES (Feb. 17, 2017, 12:02 AM), https://www.forbes.com/sites/kalevleetaru/2017/02/17/how-twitters-new-censorship-tools-are-the-pandoras-box-moving-us-towards-the-end-of-free-speech/#45f47d2bc1e4 (discussing Twitter's efforts to censor unacceptable speech).

[82] *See, e.g.*, Jessica Guynn, *Twitter Suspends Alt-Right Accounts*, USA TODAY (Nov. 16, 2016, 8:52 PM), http://www.usatoday.com/story/tech/news/2016/11/15/twitter-suspends-alt-right-accounts/93943194/ (discussing Twitter's suspension of accounts associated with the alt-right movement); Sarah Perez, *One of the Worst Comments Sections on the Internet is Shutting Down*, TECH CRUNCH (Feb. 3, 2017), https://techcrunch.com/2017/02/03/one-of-the-worst-comments-sections-on-the-internet-is-shutting-down/ (discussing Amazon's decision to close IMDb's discussion board due to prevalent hateful speech). Sometimes Facebook's automated monitoring of user content backfires. This has been the subject of broad public scrutiny very recently. In late 2016, its popular Safety Check feature mistakenly linked to false news stories about an explosion in Bangkok. Daniel Victor, *Facebook's Safety Check, Now Automated, Turns a Firecracker into an Explosion*, N.Y. TIMES (Dec. 29, 2016), http://www.nytimes.com/2016/12/29/world/asia/facebook-safety-check-bangkok.html?_r=0. The reported explosion actually occurred in the preceding year. Facebook's News Feed and Trending features also have come under fire in the United States for promoting and circulating "fake news." The company has implemented fixes for both, with fact-verification techniques drawing the most attention. *See* Amber Jamieson & Olivia Solon, *Facebook to Begin Flagging Fake News in Response to Mounting Criticism*, GUARDIAN (Dec. 15, 2016, 3:05 PM), https://www.theguardian.com/technology/2016/dec/15/facebook-flag-fake-news-fact-check (discussing Facebook's efforts to fairly and accurately fact check news reports).

regard is anything but passive.

But moderation can only go so far in regulating online content and conduct. It is, after all, mostly just reactive. This is where application design matters. It is one thing for a provider to take down user content that is inconsistent with content guidelines after it is has been posted. It is another thing altogether to design the application to elicit or shape user content or, conversely, ensure that certain kinds of content never see the light of day. Application designs determine the form and substance of user content.[83]

Consider the ways in which intermediaries that allow users to post material anonymously or pseudonymously are likely to host abusive or objectionable content.[84] Users who post harmful or illegal content reasonably assume that anonymity and pseudonymity safeguard them from shame and rebuke.[85] In this way, such design features have much to commend them. They disinhibit users from the censorship of "political correctness." They embolden users to articulate ideas and views that they would otherwise keep silent.

Application design, of course, also directly determines the form by which users express themselves. Twitter, for example, defines the way in which its users communicate. Users may communicate through tweets that now must be no more than 280 characters long for distribution to either followers or to the public at large.[86] The service, moreover, enables users to retweet others' 280-character missives or "embed" others' tweets in other applications.[87] Or users may share ideas through direct messages to discrete Twitter users.[88] Twitter optimizes all of this activity for use on

---

[83] *Cf.* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 508–09 (1999) (explaining how software design can regulate user conduct).

[84] *See, e.g.*, Jones v. Dirty World Entm't Recordings, LLC, 755 F.3d 398, 402–03 (6th Cir. 2014) (describing how Dirty World obtained stories and gossip from anonymous users). Survey data strongly suggests that online harassment is pervasive. A Pew Research Center study found, for example, that almost three-quarters of American adult internet users had witnessed online harassment and that two out of five had experienced it themselves. *Online Harassment*, PEW RESEARCH CENT. (Oct. 22, 2014), http://www.pewinternet.org/2014/10/23/12113/.

[85] It is unclear whether users engage or are inclined to engage in this kind of antisocial behavior online in ways that they would rarely engage in the physical world. *See, e.g.*, Lee Rainie, Janna Anderson, & Jonathan Albright, *The Future of Free Speech, Trolls, Anonymity and Fake News Online*, PEW RESEARCH CENT. (Mar. 29, 2017), http://www.pewinternet.org/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/ (discussing the difference between online and face-to-face social conduct); *see generally* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009).

[86] *New User FAQs*, TWITTER HELP CTR., https://support.twitter.com/articles/13920 (last visited Aug. 1, 2017).

[87] *FAQs About Retweets*, TWITTER HELP CTR., https://support.twitter.com/articles/77606 (last visited, Aug. 1, 2017).

[88] *New User FAQs*, *supra* note 86.

mobile devices.[89]

Contrast these design features with an online publishing platform like Medium, owned by Twitter's founders.[90] On the one hand, like Twitter, Medium leaves it to users to create and edit their own content.[91] But Medium also allows long-form content and stories that are a contrast to the characteristically punchy syntax of tweets.[92] Medium also supports its own original journalism and content.[93] (Twitter, meanwhile, mainly indexes trending news and user activity.)[94] Furthermore, Medium enables users to upvote and share content through Twitter and Facebook.[95] In all of these ways, then, we can say that Twitter is far more implicated in the user's choice of form and modes of distribution of content than Medium is. Indeed, the former's designers appear far more engaged in developing ways to enable easy and wide distribution of tweets.

Next, contrast Twitter and Medium with so-called ephemeral messaging applications like Snapchat and Confide—apps that enable users to distribute content that is only accessible to chosen recipients for a short period of time, and not, as in the case of most messaging applications, indefinitely.[96] Ephemeral messaging reflects a distinctive view about how user-generated content may (and perhaps ought to) be shared and retained. It makes the detection of illicit online conduct harder to record and, in this way, encourages users to post provocative or otherwise embarrassing content.[97]

An application's design today reflects its developers' priorities. The form in which users can communicate (short form or long form? anonymous or not?), the scope of other users to which users can distribute content (to discrete application users or the public at large?), and the availability of content over time (ephemeral messaging or not?) reflect application developers' view about how they want or expect users to

---

[89] *Notifications on Mobile Devices*, TWITTER HELP CTR., https://support.twitter.com/articles/20169887 (last visited, Aug. 1, 2017).

[90] Josh Halliday, *Twitter Founders Launch Two New Websites, Medium and Branch*, THE GUARDIAN (Aug. 15, 2012, 6:49 AM), https://www.theguardian.com/technology/blog/2012/aug/15/twitter-founders-new-branch-medium.

[91] *Id.*

[92] Drew Olanoff, *Ev Williams Takes To Medium To Discuss The True Purpose Of His New Publishing Tool*, TECH CRUNCH (Nov. 15, 2012), https://techcrunch.com/2012/11/15/ev-williams-takes-to-medium-to-discuss-the-true-purpose-of-his-new-publishing-tool/.

[93] *Id.*

[94] *New User FAQs*, *supra* note 86.

[95] Olanoff, *supra* note 92.

[96] *Frequently Asked Questions*, CONFIDE, https://getconfide.com/faq (last visited Aug. 1, 2017); Elise Moreau, *What is Snapchat? An Intro to The Popular Ephemeral App*, LIFEWIRE (June 13, 2017), https://www.lifewire.com/what-is-snapchat-3485908.

[97] Nathan Olivarez-Giles, *Instagram Takes Aim at Snapchat with Live Video and Vanishing Photos*, WALL ST. J. (Nov. 21, 2016), https://www.wsj.com/articles/instagram-takes-aim-at-snapchat-with-live-video-and-vanishing-photos-1479741171.

express themselves. Today, therefore, a provider's decision to design an application to be ostensibly agnostic about its users' illicit content or online behavior suggests passivity. But it also conveys the knowing expectation that users will post illegal and taboo online content.[98]

This is to say that, today, online intermediaries are not mere conduits that purport to provide a free and uninhibited forum for social interaction. They are implicated in every user utterance or act, even if they do not moderate posts.

### C. *Antisocial Designs*

But we can go even further in our account of service or application designs. Sometimes, as I suggest above, developers' designs encourage user content that causes material injury, as in the case of the Twitter user who sent a direct message containing an animated strobe-light effect to a journalist known to suffer from epilepsy.[99] It is in spite of these potential harms, however, that the social media company enables its users to disguise their identities. Twitter does so in the interest of cultivating a forum for uninhibited online interaction, knowing all along someone will inevitably get hurt.

Anonymity or pseudonymity can be dangerous. Other application designs also facilitate predictable harms. Consider the way in which users search for rides and guests through ride-sharing applications and short-term homestay marketplaces. One recent study found that African-American passengers in Seattle wait up to 35-percent longer for

---

[98] There are some providers that have remained indifferent if not altogether defiant about hosting illicit or otherwise objectionable third-party content. These companies purport to do nothing more than connect users, many of whom happen to have objectionable tastes. While large providers like YouTube or Facebook may be wary of broad consumer distaste for objectionable content that passes through their applications, others are not because there is monetizable demand for it. Such a provider can create an adults-only or otherwise restricted platform through which users may trade and share taboo or objectionable material. But such a service would likely not last long. Consider Craigslist, the online classified site. It closed its adults-only section in 2010 after a series of shocking events arising from advertisements and solicitations on the site. Claire Cain Miller, *Craigslist Says It Has Shut Its Section for Sex Ads*, N.Y. TIMES (Sept. 15, 2010), http://www.nytimes.com/2010/09/16/business/16craigslist.html. BackPage soon picked up where Craigslist left off, but its adults-only section did not last long after revelations about the way in which its users engaged in sex trafficking of minors. Matt Hamilton, *BackPage Shuts Down Adult Section, Citing Government Pressure and Unlawful Censorship Campaign*, L.A. TIMES (Jan. 9, 2017), http://www.latimes.com/local/lanow/la-me-ln-backpage-shutdown-20170109-story.html.

[99] *See, e.g.*, Eriq Gardner, *Newsweek Writer Going After Twitter User for Allegedly Causing Seizure*, HOLLYWOOD REPORTER (Dec. 19, 2016), http://www.hollywoodreporter.com/thr-esq/newsweek-writer-goes-twitter-user-allegedly-causing-seizure-957631 (reporting on Newsweek writer Kurt Eichenwald's suit against a Twitter user who allegedly sent him an email intending to cause a seizure); Ana Silman, *A Timeline of Leslie Jones's Horrific Online Abuse*, N.Y. MAG. (Aug. 24, 2016), http://nymag.com/thecut/2016/08/a-timeline-of-leslie-joness-horrific-online-abuse.html (reporting on the viciously racist and sexist internet trolling of actress and comedian Leslie Jones).

Uber cars than white passengers.[100] The researchers attributed the longer wait time to drivers who cancel trips upon hearing that the passenger has an "African American sounding first name."[101] Male passengers who requested a ride from a low-density area, moreover, were more than three-times as likely to have the Uber driver cancel the trip when the passenger uses an African-American-sounding name as compared to a white-sounding name.[102]

An even more publicized survey by scholars at Harvard Business School reported similar findings in its review of rental booking patterns on Airbnb, the homestay sharing application.[103] According to the report, Airbnb guests "with distinctively African-American names are 16-percent less likely to be accepted relative to identical guests with distinctively White names."[104] Airbnb's own study on the topic found, moreover, that hosts discriminate against racial minorities whose profile pictures ostensibly present themselves as such.[105]

In the case of Uber and Airbnb, the choice to publicize personal information through names and pictures is a design choice. In the case of Airbnb in particular, user pictures are meant to engender a sense of authenticity and connection among hosts and guests.[106] (This is in contrast to the authenticity that Twitter seeks to engender through pseudonymity.) But, of course, it is in this same way that Uber drivers and Airbnb hosts might eschew connections with people with whom they feel less comfortable on the basis of racist stereotypes. The features that mean to foster authentic connection also reinforce bias and exclusion.

Facebook offers a compelling illustration of this point as well. The online social networking application is well-known for its mission to connect the world.[107] With this ambition in mind, the company has invested a substantial amount of resources into developing features (e.g., the scrolling News Feed or Trending feature) and services (e.g., Free Basics) that are meant to keep users connected.[108]

---

[100] Yanbo Ge et al., *Racial and Gender Discrimination in Transportation Network Companies* 2 (Nat'l Bureau of Econ. Research, Working Paper No. 22776, 2016).

[101] *Id.* at 11–12.

[102] *Id.* at 19.

[103] Edelman et al., *supra* note 18, at 2.

[104] *Id.* at 1.

[105] MURPHY, supra note 21, at 16–17.

[106] *Id.* at 11, 17.

[107] Associated Press, *Zuckerberg's Goal: Remake a World Facebook Helped Create*, L.A. TIMES (Feb. 17, 2017), http://www.latimes.com/business/la-fi-tn-zuckerberg-vision-20170217-story.html.

[108] *See* Newsroom, *A New Look for News Feed*, FACEBOOK (Mar. 7, 2013), http://newsroom.fb.com/news/2013/03/a-new-look-for-news-feed/ (discussing new features of the Facebook News Feed design implemented in 2013); *see also* Facebook For Developers, *What's Free Basics?*, FACEBOOK, https://developers.facebook.com/docs/internet-org (last visited Aug. 1, 2017) (describing the Free Basics service which provides basic internet functionality to a billion people across

Ostensibly in keeping with this practice, the company launched an advertising service in 2014.[109] Through it, advertisers may "microtarget" small or fleeting niche audiences that might otherwise be hard to reach.[110] Facebook assigns an "affinity" designation by applying proprietary tools for algorithmic analysis to its vast reserve of user data.[111] The company forms the affinities around a particularly salient bundle of user data.[112] The users to whom the advertisements are distributed play no active role in determining the designations that Facebook assigns them.[113] They only need to keep liking, sharing, scrolling, and building friend networks—that is, they only need to continue using the social media application.[114]

Controversially, Facebook's service offers "ethnic affinities" as a category which advertisers can use to microtarget their campaigns.[115] Through the advertising service, a hypothetical business manager could distribute ads for a rental unit to users with an African-American "ethnic affinity" or, just as easily, exclude such users from the advertisement. Employers, too, could use the service to look for new recruits, again, singling out users for inclusion or exclusion based on the category designation.

While the advertising service has been available since 2014, ProPublica's reporting on this feature of the service in late 2016 drew a lot of attention.[116] Public reaction to the report was mixed, if not altogether negative.[117] Within one month, Facebook discontinued the "ethnic affinity" designation and clarified its privacy and advertising policy to

---

Latin America, Africa, and Asia); Vadim Lavrusik, *How the New News Feed Design Improves Content Discovery*, FACEBOOK (Mar. 7, 2013), https://www.facebook.com/notes/journalists-on-facebook/how-the-new-news-feed-design-improves-content-discovery/571743776170974/ (discussing the introduction of categorized and real time content feeds to the Facebook News Feed design in 2013).

[109] Alex Hern, *Facebook Is Trying to Explain How Its New 'Ethnic Affinity' Ads Aren't Really Racial Profiling*, BUS. INSIDER (Mar. 22, 2016, 10:57 AM), http://www.businessinsider.com/facebook-trying-to-explain-its-new-ethnic-affinity-ads-2016-3.

[110] Angwin & Parris, *supra* note 16.

[111] *Id.*

[112] *See* Hern, *supra* note 109 (stating that "liking" certain racially-coded pages indicates a user's ethnic affinity).

[113] *Id.*

[114] *Id.*

[115] Angwin & Parris, *supra* note 16.

[116] *Id.* Following the ProPublica reporting, numerous other news outlets picked up the story. A Google search for derivative coverage yields more than a dozen other articles citing the ProPublica reporting. Search Query, GOOGLE, www.google.com (search "ProPublica Facebook article ethnic affinity microtargeting").

[117] The report could not have come at a worse time for Facebook, as the social media company was also defending against separate allegations that the company engaged in viewpoint censorship, secretly collaborated with law enforcement to surveil users, and did not moderate fake news.

make plain that it does not approve of racial discrimination.[118] It later launched a new "multicultural affinity" filter, ostensibly to be less equivocal about the original classification.[119] ("Multicultural" presumably connotes something more positive.) These reforms, however, were not enough to stop aggrieved users from filing a class-action lawsuit in the Northern District of California against Facebook (and brokers and lessors) in late 2016. Plaintiffs allege that, through the advertising service, Facebook enables users to discriminate against prospective renters and employers in violation of the federal FHA and antidiscrimination in employment provisions of Title VII of the Civil Rights Act.[120] One year later, Facebook reportedly continues to enable discrimination against protected classes under the FHA.[121]

Facebook has three overlapping answers to the charge that it was or is violating the FHA. First, it observes that it is common for advertisers to target audiences in exactly the way that it did with the "ethnic affinities" feature.[122] The fragmented and diverse nature of the market makes it important for advertisers to know their audience with more granularity.[123] Thus, it argues, it is unremarkable to exclude, for example, the "Hispanic affinity group" from an English-language advertisement.[124] Second, Facebook argues that its policies forbid "advertisers from using the targeting options for discrimination, harassment, disparagement or predatory advertising practices."[125] The company promptly removes such

---

[118] Gillian B. White, *When Algorithms Don't Account for Civil Rights*, THE ATLANTIC (Mar. 7, 2017), https://www.theatlantic.com/business/archive/2017/03/facebook-ad-discrimination/518718/; *Improving Enforcement and Promoting Diversity: Updates to Ads Policies and Tools*, *supra* note 25.

[119] White, *supra* note 118; *Improving Enforcement and Promoting Diversity: Updates to Ads Policies and Tools*, *supra* note 25.

[120] Complaint ¶¶ 24–33, Mobley v. Facebook, Inc., No. 5:16-cv-06440-EJD (N.D. Cal. Nov. 3, 2016), 2016 WL 6599689. The federal FHA forbids home sellers or renters from distributing advertisements "that indicate[] any preference, limitation, or discrimination based on race, color, religion, sex, handicap, familial status, or national origin." 42 U.S.C. § 3604(c) (2017). The law also, of course, forbids discrimination on the basis of those characteristics as well. *Id.* § 3604(b). The statute also provides that it is unlawful "to discriminate against any person in terms, conditions, or privileges of sale or rental of a dwelling" along those demographic dimensions. *Id.* Among other things, Title VII of the Civil Rights Act makes it unlawful for an employer "(1) to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin; or (2) to limit, segregate, or classify his employees or applicants for employment in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual's race, color, religion, sex, or national origin." 42 U.S.C. § 2000e-2(a) (2017).

[121] See Julia Angwin, Ariana Tobin, and Madeleine Varner, *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, PROPUBLICA (Nov. 21, 2017), https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin?utm_campaign=sprout&utm_medium=social&utm_source=twitter&utm_content=1511288776.

[122] Angwin & Parris, *supra* note 16.

[123] *Id.*

[124] *Id.*

[125] *Id.*

ads (and perhaps even suspends or terminates accounts of violators) when it receives notice of them.[126] Third, Facebook does not concede that "ethnic affinity" is protected under fair housing law.[127] That designation "is not," it argued, "the same as race."[128] It only represents an algorithmic judgment based on a mix of salient user data, in the same way, for example, that age, relationship status, employment history, or page-like patterns may suggest something about a user's inclination to shop.

We can assume for the purposes of argument that Facebook's reasons for offering the advertising service are not overtly racist. Nor does it seem that its design choices to identify "ethnic affinity" and enable advertisers to affirmatively exclude (as opposed to include) audiences on that basis were meant to discriminate against racial minorities.[129] Facebook launched the advertising service presumably to leverage its social network in other lines of business. In this case, Facebook probably believed that its distinctively powerful capacity to process and sort user data could enlarge users' communicative capacity. Facebook, under this view, was only acting as a mere conduit between advertisers and users.

But such an approach is either naïve or careless or worse. It was predictable to the point of being inevitable that advertisers would use Facebook's "ethnic" or "multicultural affinity" classifications to discriminate against people of color. Today, race overdetermines the distribution of material resources in this country to the systemic detriment of people of color. Well-documented patterns of racial discrimination online prove the point. A Stanford study from 2010 found that black sellers receive fewer offers and less money than white sellers when the seller's race is evident in an accompanying photo.[130] Consider, moreover, the ways in which users discriminate against blacks on online dating sites like Match. Or consider crowdsourced neighborhood safety rating applications like the now-defunct SketchFactor that served as little more than a platform for racist stereotypes about "shady" parts of town.[131]

This recent Facebook advertising episode just underscores that, in its purported role as conduit between advertisers and buyers, Facebook facilitates material bias against disfavored groups. More pertinently, it

---

[126] *Id.*

[127] *Id.*

[128] *Id.*

[129] For equal protection and civil rights enforcement, Facebook's intentions would matter a great deal.

[130] *See* Louis Bergeron, *Online Shoppers More Likely to Buy from White Sellers than Black, Stanford Researchers Say*, STANFORD NEWS (July 19, 2010), http://news.stanford.edu/news/2010/july/hands-craigslist-study-071910.html (discussing research later published in Jennifer L. Doleac & Luke C.D. Stein, *The Visible Hand: Race and Online Market Outcomes*, 123 ECON. J. 469 (2013)).

[131] Andrew Marantz, *When an App Is Called Racist*, NEW YORKER (July 29, 2015), https://www.newyorker.com/business/currency/what-to-do-when-your-app-is-racist.

illustrates that ostensibly passive application design is far more generative of bad behavior than the Section 230 doctrine adequately addresses. This recent controversy raises questions about the scope of immunity under Section 230 as it relates to application design.[132] But, before saying more, it is important to understand the current immunity doctrine and how it came to take this form. I turn to that next.

## II. THE PREVAILING IMMUNITY DOCTRINE

Courts have read Section 230 broadly on the theory that online intermediaries should not be held liable if, as publishers, they are mere conduits for user-generated content. The current doctrine specifically provides that intermediaries are only liable if they materially contribute to the illegal or otherwise objectionable online conduct.[133] Courts reason that online entrepreneurship and speech would be chilled if providers had the heavy burden of policing their users' online content.[134] In this Part, I explain the manner in which the courts have come to this standard. This analysis also offers important lessons on whether the doctrine has anything to say about the duties intermediaries owe for their designs. Could courts apply the material contribution standard to each design? If so, how affecting must that design be in order for an intermediary to be liable for the unlawful conduct of its third-party users?

---

[132] We can expect Facebook to invoke Section 230 in its defense of the Northern District of California suit. The company has not been shy about relying on that provision in other cases addressed to the illegal behavior of third-party Facebook users. *See, e.g.*, Klayman v. Zuckerberg, 753 F.3d 1354, 1357 (D.C. Cir. 2014) (holding that Section 230 mandated dismissal of the plaintiff's negligence claims against Facebook); Finkel v. Facebook, Inc., No. 102578/09, 2009 WL 3240365 (N.Y. Sup. Ct. Sept. 15, 2009) (dismissing a defamation action against Facebook, again due to its immunity from suit under Section 230).

[133] *See* Jones v. Dirty World Entm't Recordings, 755 F.3d 398, 408 (6th Cir. 2014) ("[I]f a website operator is in part responsible for the creation or development of content, then it is an information content provider as to that content—and is not immune from claims predicated on it." (citation omitted)).

[134] *Id.* at 407, 417.

### A. *The Statutory Text*

The pertinent provision, 47 U.S.C. § 230(c), is entitled "Protection for 'Good Samaritan' Blocking and Screening of Offensive Material."[135] The plain language is relatively straightforward. Section 230(c)(1), whose subtitle is "Treatment of publisher or speaker," 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."[136] Under the statute, an "interactive computer service" mainly denotes services that "provide[] access to the Internet."[137]

Section 230(c)(1) does far more work than its plain language suggests. The term "publisher or speaker" refers to an entity that participates in or authorizes the publication of content.[138] It is generally associated with the claim for defamation, which, to be successful, requires evidence of the intentional or negligent publication of defamatory material about a plaintiff to a third person.[139]

Under the "republication rule" in defamation law the duties of a "publisher" are especially important. A publisher, the rule holds, is strictly liable for repeating defamatory statements by third parties to the extent the publisher intentionally circulates the material or just fails to take reasonable care to prevent its publication.[140] Publishers in this scheme include book publishers, newspapers, radio or television stations, and other entities that exercise editorial control over the content that they publish.[141] A publisher is in this way just as liable for circulating the defamatory statements as the entity who originally authored them.[142] The rule exists to protect others from the harm done by the repeated distribution of an illegal

---

[135] 47 U.S.C. § 230(c) (2017).

[136] *Id.* § 230(c)(1).

[137] The pertinent definition of "interactive computer service" under the statute is as follows: "[A]ny 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." *Id.* § 230(f)(2).

[138] Barrett v. Rosenthal, 146 P.3d 510, 520 (Cal. 2006) ("Those terms, employed in section 230(c)(1), are drawn from the law of defamation."). There are reasons to doubt that defamation should be our guide, at least because the provision here refers to "publisher *or speaker*," the latter not being tied to defamation doctrine. *See id.* at 513 (emphasis added) (providing a statement by Congress in the Communications Decency Act of 1996).

[139] *See* RESTATEMENT (SECOND) OF TORTS § 577(1) (AM. LAW INST. 1977).

[140] *See id.* § 578; *see also* W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 113 (5th ed. 1984) (detailing the basis of liability).

[141] *See* RESTATEMENT (SECOND) OF TORTS § 568A; *id.* § 577A.

[142] *See id.* § 578. *See generally* Benjamin C. Zipursky, Lecture, *Online Defamation, Legal Concepts, and the Good Samaritan*, 51 VAL. U. L. REV 1 (2016) (performing a thorough analysis of republication rule).

utterance.[143] Without the rule, the logic goes, "defamers could too easily sidestep any possible liability by putting words into another's mouth."[144]

The old common law rule carved out a species of publisher that distributes or otherwise "deliver[s] or transmit[s]" defamatory material published by a third person.[145] These distributors, as they are called in the doctrine, are only liable to the extent they know or have reason to know that the material is illegal.[146] That is, they are subject to notice liability. Conventional examples of distributors are newsstands and bookstores.[147] A distributor, under this view, could not be liable for distributing a user's defamatory statement about a third party unless the aggrieved party could show that the distributor's failure to know of the defamatory nature of the statement was negligent or that the distributor failed to remove the material once it gained knowledge of it.[148] Publishers, on the other hand, could be liable whether they know the material is defamatory or not.

Section 230(c)(1) reforms the old common law by effectively shielding providers of "interactive computer services" from liability for content that third-party users circulate through the online service.[149] The statute further clarifies the extent of this immunity in its definition of "information content provider," which it describes 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."[150] With this, a provider could be liable for content that appears on its service to the extent the provider actively helps in the "creation or development" of the objectionable material.[151]

Alone, this reform of the republication rule would be significant. Section 230(c)(1) shields service providers from liability for exercising editorial judgment about content. A service will only be liable to the extent it is responsible at least in part for the "creation or development" of the content that it publishes.[152]

---

[143] *See* RESTATEMENT (SECOND) OF TORTS § 576; *id.* § 577.

[144] Zipursky, *supra* note 142, at 5.

[145] RESTATEMENT (SECOND) OF TORTS § 578; *see also* Church of Scientology of Minn. v. Minn. State Med. Ass'n Found., 264 N.W.2d 152, 156 (Minn. 1978) ("Those who merely deliver or transmit defamatory material previously published by another will be considered to have published the material only if they knew, or had reason to know, that the material was false and defamatory.").

[146] RESTATEMENT (SECOND) OF TORTS § 581; *see also* Barrett v. Rosenthal, 146 P.3d 510, 513 (Cal. 2006) ("Under the common law, 'distributors' like newspaper vendors and book sellers are liable only if they had notice of a defamatory statement in their merchandise.").

[147] *Barrett*, 146 P.3d at 513.

[148] RESTATEMENT (SECOND) OF TORTS § 577(2).

[149] 47 U.S.C. § 230(c)(1) (2017). The statute explicitly preempts state tort law. Section 230(e)(3) provides, among other things, that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." *Id.* § 230(e)(3).

[150] *Id.* § 230(f)(3).

[151] *Id.*

[152] *Id.*

As significant as the reform in Section 230(c)(1) is, a couple subsequent provisions do more. Section 230(c)(2), entitled "Civil liability,"[153] takes up Section 230(c)'s evocative "Good Samaritan"[154] title in ways that Section 230(c)(1) does not.[155] Quite unlike Section 230(c)(1), Section 230(c)(2) identifies specific circumstances for applying the immunity: that is, when an interactive computer service takes steps in good faith to take down objectionable material or help others to do so.[156] This immunity presumably exists for blocking and removing constitutionally protected material like core political speech as well as speech like defamation or obscenity that is not protected.[157] Section 230(c)(2), moreover, shields interactive computer services to the extent they "enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)."[158]

Section 230(d), the following subsection, obliges interactive computer services to inform their users that "computer hardware, software, or filtering services" exist to "limit[] access to material that is harmful to minors."[159] This provision does not come paired with an enforcement mechanism. Nor, for that matter, do Sections 230(c)(1) or 230(c)(2)(A). But those two latter provisions operate as affirmative defenses, to be invoked by interactive computer services in litigation. Section 230(d), on the other hand, reads as little more than a strongly worded but unenforceable mandate.

In any event, both (c) and (d), and especially the former, presume that voluntary market-driven norms will guide the regulation of objectionable online content rather than government enforced mandates. They depend on interactive computer services for their implementation. While the online setting has been relatively new to the common law, the challenge of encouraging (without requiring) good deeds through law is not.[160] The Good Samaritan statutes in the states long preceded the internet.[161] Through these, state legislatures sought to balance competing considerations in ways that are instructive. On the one hand, the states

---

[153] *Id.* § 230(c)(2).

[154] *Id* § 230(c).

[155] The latter makes no allusion at all to the biblical parable. *See Luke* 10:25–37.

[156] Section 230(c)(2) shields interactive computer services that have voluntarily taken steps in good faith to censor or take down "material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected." 47 U.S.C. § 230(c)(2)(A).

[157] *Id.*

[158] *Id.* § 230(c)(2)(B).

[159] *Id.* § 230(d).

[160] *See, e.g.*, RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008).

[161] Zipursky, *supra* note 142, at 31.

have wanted to encourage strangers to help victims. On the other, the common law does not impose duties to help strangers in need.[162] Instead, do-gooders can be liable under common law for causing injuries that arise from their efforts to treat down-and-out strangers with kindness.[163] Thus, in the face of a common-law rule that arguably disincentivizes the Good Samaritan, state legislatures have passed laws that one way or another shield defendant do-gooders from liability.[164]

Section 230(c)(2) embodies this same effort, but in the online setting. It ostensibly aims to preserve the affirmative duty to restrict access to objectionable content to the extent the defendant service at issue "has undertaken to" do so.[165]

This approach distinguishes Section 230 from most other provisions addressed to illegal or objectionable content in the Communications Act. Other parts of the statute, for example, strictly bar the transmission of obscenity, child pornography, or harassing content and, moreover, explicitly enlist officials at the Department of Justice and the Federal Communications Commission to impose financial penalties on violators and bring criminal and civil forfeiture actions.[166] In contrast, government regulators play no part in monitoring and regulating content that users share over the internet through "interactive computer services."[167]

## B. *Legislative Intent*

### 1. *Prefatory Words*

It is not easy to balance the interest in promoting user-generated content against the voluntary regulation of objectionable online content. But that is exactly what the drafters of Section 230 purported to do. Congress explicitly set out the findings and policies on which it based the immunity in Sections 230(a) and (b). The internet, the statute asserts, affords users "a great degree of control over" the "extraordinary" array of "educational and informational resources" they receive.[168] This finding restates one of the foundational design principles of the internet: that the substantive intelligence of information networks should reside with end-

---

[162] *Id.*

[163] *Id.*

[164] *Id.*

[165] *Id.* at 35.

[166] *See* 47 U.S.C. §§ 223(a), 223(b)(6) (2017) (discussing prohibited acts and the Attorney General's authority to enforce the statute); 18 U.S.C. § 1464 (2017) (discussing prohibitions against the broadcasting obscene language).

[167] *See* 47 U.S.C. § 230(c)(1) (2017) (stating that users of an interactive computer service will not be considered a "publisher or speaker" of any information provided by another information content provider).

[168] 47 U.S.C. §§ 230(a)(1)–(3).

users and not, as had been the case, in the central offices of newspaper publishers or broadcast producers, for example. This approach jibes, too, with an emergent liberal political theory with which this engineering concept is often associated.[169] Indeed, along these lines, Congress observed in their statutory findings that the internet is a "forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[170] This statutory recital has been an article of faith among policymakers and lay observers, at least since the Supreme Court's first prominent take on the technology two decades ago.[171] Congress also found in this section that the "variety of political, educational, cultural, and entertainment services" online have "flourished . . . with a minimum of government regulation."[172]

Section 230(b) enumerates the policies underlying the protection for intermediaries. There, legislators provide that the statute's aim is "to promote the continued development of the Internet and other interactive computer services and other interactive media";[173] "preserve the vibrant and competitive free market . . . unfettered by Federal or State regulation";[174] and to "maximize user control over what information is received by individuals, families, and schools," which includes encouraging "the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material . . . ."[175] Finally, through Section 230, Congress sought "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer."[176]

As clear as these introductory provisions are, courts have yet to cohere them (at least explicitly) with the legislative purpose that the New Deal-era Congress explicitly set out in Section 151 of the Communications Act, the first provision of the statute that Section 230 amends.[177] That older provision mainly provides that the purpose of the statute is "to ensur[e] that communication technology is widely available to all users irrespective of

---

[169] *See* YOCHAI BENKLER, WEALTH OF NETWORKS 133 (2006) (discussing individual agency, technology, and the rights of end-users versus publishers and broadcasters).

[170] 47 U.S.C. §§ 230(a)(1)–(3).

[171] *See* Reno v. ACLU, 521 U.S. 844, 849–850 (1997) (discussing the role of the internet and how access provides opportunities to users).

[172] 47 U.S.C. §§ 230(a)(4)–(5).

[173] *Id.* § 230(b)(1).

[174] *Id.* § 230(b)(2).

[175] *Id.* § 230(b)(3)–(4).

[176] *Id.* § 230(b)(5).

[177] 47 U.S.C. § 151 (2012); *see also* Comcast Corp. v. FCC, 600 F.3d 642, 652–654 (D.C. Cir. 2010) (rejecting the argument that Sections 151 and 230 authorized the agency action at issue).

who or where they are."[178] This language is not in tension with the "findings" or "policy" underlying Section 230. It nevertheless suggests that, to the extent courts attend to the statutory purposes of Section 230, they would do well to consider the distributional interests that rest at the heart of the Communications Act, of which Section 230 is just a part.

2. *Legislative History*

These prefatory terms are notable for their clarity.[179] But they are especially valuable because the legislative history of Section 230 is relatively spare on what Congress meant to accomplish with the statute. To the extent the legislative history suggests anything, it does not square easily with all of the plain language.

The bill that would become Section 230 was part of a much larger legislative reform of communications law addressed in particular to competition in the market for last-mile telecommunications service.[180] Senators James Exon and Slade Gorton introduced the bill, Title V of the proposed Telecommunications Act, to the Senate Committee of Commerce, Science, and Transportation.[181] Among other things, the Exon-Gorton bill contained government-enforced restrictions on indecent and obscene online speech, as well as the enforcement provisions to which I allude above.[182] But it also included two new defenses to liability: first, an immunity for providers that only supply internet access and, second, an immunity for providers that take good-faith efforts to prevent third-party users' publication of obscene or indecent material.

The House bill that went to conference also contained an immunity provision.[183] But Representatives Christopher Cox and Ron Wyden only moved to include it after the House Energy and Commerce Committee had already reported the pertinent bill out to the full chamber without one.[184] Cox and Wyden intended their proposed language to be an alternative to

---

[178] Sylvain, *supra* note 43, at 459.

[179] *See Comcast Corp.*, 600 F.3d at 652–54 (discussing statutory terms and the areas over which the FCC has authority); Verizon v. FCC, 740 F.3d 623, 645 (D.C. Cir. 2014) (discussing statutory terms and the areas that fall within the purview of the FCC).

[180] *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (enacting the Communications Decency Act as Section V of the overall reform act).

[181] *See* 141 CONG. REC. S1953 (daily ed. Feb. 1, 1995) (statement of Sen. Exon) (introducing the Communications Decency Act on behalf of himself and Senator Gorton).

[182] *See* Reno v. ACLU, 521 U.S. 844, 864 (1997) (striking down obscenity and indecency laws within one year of their implementation).

[183] *See* 104 CONG. REC. H8469 (statement of Rep. Cox) (reading the proposed amendment, which contained a Good Samaritan immunity provision).

[184] *See id.* at H8468 (statement of Rep. Cox) (offering an amendment after the reading of the bill to include the Good Samaritan provision, in addition to others).

the Exon-Gorton language.[185] Its main purpose was to overrule a 1995 New York state trial court opinion that had found Prodigy, an early online service, liable for defamatory statements made by another user on one of the service's bulletin board services.[186] Relying on the common law regarding publisher liability, that court had decided that Prodigy was a "publisher" and, thus, just as liable for libelous statements made by any of its subscribers. The court explained, moreover, that Prodigy had marketed itself as having editorial control over the content that flowed through its service and, as a result, should be held to account for failing to remove the offending content.[187]

Representatives Cox and Wyden saw the *Prodigy* opinion as a dangerous incursion on the free flow of information online.[188] They, as with the then-nascent internet industry, believed that the opinion would open the door to litigation against well-meaning services. The Cox-Wyden bill sought to encourage private "Good Samaritan" providers like Prodigy to filter objectionable content without fear of punishment for doing so ineffectively.[189] Above all, Cox and Wyden proposed the bill as an alternative to direct government restrictions on speech, believing that "parents and families are better suited to guard the portals of cyberspace and protect our children than our Government bureaucrats."[190] Under the approach set out in their amendment, they explained, "the marketplace is going to give parents the tools they need," while the alternative set out by the Senate bill would "set back the effort to help our families."[191]

---

[185] *See id.* at H8470 (statement of Rep. Cox) (comparing their approach with that of "other ways to address this problem"); *id.* (statement of Rep. Wyden) (noting that their proposal language in the House "stand[s] in sharp contrast to the work of the other body").

[186] *See id.* (statement of Rep. Cox) (discussing the purposes of the proposed amendment).

[187] *See* Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, at *2 (N.Y. Sup. Ct. May 24, 1995), *superseded by* 47 U.S.C. § 230(c)(1), *as recognized in* Shiamili v. Real Estate Group of New York, Inc., 17 N.Y.3d 281 (2011).

[188] *See* 141 CONG. REC. H8460 (1995) (statement of Rep. Cox.) (discussing disincentives that exist in the legal system that prevent free-flowing online information).

[189] *See id.* (discussing the protection of Good Samaritans, online service providers that take steps to screen offensive material for customers).

[190] *Id.* (statement of Rep. Wyden); *see also id.* (statement of Rep. Cox) ("[The proposed bill] will establish as the policy of the United States that we do not wish to have content regulation by the Federal Government of what is on the internet, that we do not wish to have a Federal Computer Commission with an army of bureaucrats regulating the internet because frankly the internet as grown up to be what it is without that kind of help from the Government. In this fashion we can encourage what is right now the most energetic technological revolution that any of us has ever witnessed.").

[191] *Id.* Their justification was (and remains) at odds with the federal courts' holding that direct government regulation of indecency and obscenity furthers the government's compelling interest in parental control of the information to which children are exposed. *See, e.g.*, Sable Communications v. FCC, 492 U.S. 115, 119 (1989) (discussing the government's interest in protecting users of online service providers from indecent material); FCC v. Pacifica, 438 U.S. 726, 749 (1978) (discussing the government's interest in protecting the well-being of online service providers by regulating protected expression); Ginsburg v. New York, 390 U.S. 629, 629 (1968) (discussing the use of government

The conference committee bill that both chambers approved incorporated the Cox-Wyden formulation.[192] The accompanying report explained that "one of the specific purposes" of the amendment was to overrule the *Prodigy* opinion in order to further the "important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services."[193] This statement of purpose underscores that legislators mainly chose against a flat-out restriction on objectionable material. The drafters believed that parents are the better stewards of the online content that their children consume than governmental officials.

But neither the conference committee report nor legislators' statements about the amendment reveal anything about the scope of notice liability for service providers or the affirmative duty of interactive service providers to screen objectionable content. That is, neither says anything about how proactively interactive computer services like Prodigy must monitor third-party users' content on their services or filter out objectionable material under the new law.

We might assume that this silence suggests that the amendment immunizes all providers from any liability arising from third-party content. But this is hard to square with a plain reading of the statute. Section 230(c)(2)(A) encourages websites to keep objectionable content out without fear of liability for failing to do so well. The following provision, Section 230(c)(2)(B), immunizes services that "make available to information content providers or others the technical means to restrict" objectionable content. The plain language of (c)(2) suggests that these are the operative reasons for immunity.[194]

The legislative history also offers little in the way of explanation for these specific provisions. Again, the history only *suggests* that Congress did not want the *Prodigy* court's unforgiving interpretation of the republication rule in the online setting to stand. To the extent members said anything about the bill, it was that they were interested in enacting a statutory scheme that would empower parents to monitor their children's access to online content over a scheme that encouraged or even required websites to assume that responsibility.[195] This stated purpose does not help

---

regulations to protect minors from harmful material). The scheme that Cox and Wyden laid out invoked the parental control rationale to remove government speech regulation.

[192] *See* 142 CONG. REC. S687, S688 (daily ed. Feb. 1, 1996) (discussing the passage of the bill by the two houses).

[193] TELECOMMUNICATIONS ACT OF 1996, H.R. Rep. No. 104-58, at 194 (1996).

[194] 47 U.S.C. §§ 230(c)(2)(a)–(b) (2012).

[195] *See Pacifica*, 438 U.S. at 758 (discussing the trend in Constitutional interpretation recognizing parents' authority to decide what negative content children are exposed to); *Ginsburg*, 390 U.S. at 639 (describing the parents' authority to direct the rearing of their children as basic in the structure of our society).

shed light on whether services that *do not* take steps in good faith to filter out objectionable content (firms *unlike* Prodigy) are entitled to the immunity under Section 230. Consider that, four years before the state court weighed in, a U.S. District Court for the Southern District of New York had ruled that a similar service, CompuServe, could not be held liable to the extent it did not market or distribute defamatory material by third-party users.[196]

Congress only further complicated things when, in 1998, it amended Section 230 (for the first and last time) with a new subsection (d) which, as I explain above, requires providers to inform their users about filtering technologies.[197] This requirement is mostly toothless, as Congress did not pair it with an enforcement mechanism. And it only appears to be addressed to the kind of unprotected content that the courts and policymakers believe harms children (i.e., obscenity and indecency), not all other categories of objectionable or illegal speech. So, while it reinforces the view that Congress was primarily focused on making parents the stewards of the information that their children receive online on the one hand, the provision does not explain how far providers must go or whether immunity under Section 230(c) is conditioned on giving notice to users about parental control protections.

### C. *Statutory Ambiguities*

The thinness of the legislative history on service providers' affirmative duties to moderate content under Section 230 created an opening for litigants. There is little question that Congress sought to "modernize" the republication rule in the final language. But how far did the reform go? The exact scope of protection under the plain terms of the provision is not evident from the text and the legislative history teaches us little. In order to know whether it covers application design, however, the answer to that question is important if not dispositive.

#### 1. *Which Torts?*

We do not know from its text, for example, whether Section 230(c) immunizes service providers from all tort liability arising from third-party user content. On the one hand, Section 230(c)(1) is unequivocal, asserting without qualification that "No provider or user of an interactive computer service shall be treated as a publisher or speaker of any information

---

[196] Cubby v. Compuserve, 776 F. Supp. 135, 143 (S.D.N.Y. 1991).

[197] *See supra* Section II.A (discussing a lack of an explicit enforcement mechanism in the language of the statute).

provided by another information content provider."[198] This presumably covers all torts arising from expressive acts by third parties.

But there is also enough in the statute to limit the scope of the protection to publisher liability in defamation law, as well as liability for publishing third-party indecency and obscenity. First, the question of whether a service may be treated as a "publisher or speaker" is specific to the doctrine of defamation. It is not germane to other torts like fraud or unfair competition. Nor is it clear whether this sense of "publisher" includes notice liability normally associated with distributors in defamation law. Courts could just decide that the statute does not reach further than publisher liability for defamation or other reputational torts, thus exposing distributors and others to liability. Second, if the legislative history of Section 230(c) teaches anything certain, it is that Congress sought to overturn the *Prodigy* court's application of defamation to an online bulletin board. We can infer from this alone that defamation was the cause of action that drove Congress to act.

The only other expressive torts to which Congress explicitly turned its attention in the text are third-party communications that the courts have deemed "objectionable" or otherwise harmful to minors. Section 230(c)(2), the provision that shields Good Samaritans, and Section 230(d), the provision that imposes the obligation to notify parent users about filtering technologies, are both addressed to protecting minors from objectionable content.[199] Recall, moreover, that the original Title V amendment included flat-out restrictions on the distribution of obscenity and indecency, categories of speech from which legislators have long sought to shield children.[200] This earlier version of the bill covered nothing else. Finally, in the precatory "policy" recitation at the outset of the statute, Congress sought to encourage "individuals, families, and schools" to use "blocking and filtering technologies" to protect children from "objectionable or inappropriate online material."[201] Congress endorsed this view in Section 230(d), the 1998 amendment, by imposing an additional duty on providers to educate parents about filtering technologies.[202]

With this textual evidence, we might not read Section 230(c) as unequivocal at all, but, rather, as limiting the range of protection to providers that, on the one hand, publish third-party communications that damage a plaintiff user's reputation and, on the other hand, take good-faith steps to screen content that is "objectionable" or otherwise harmful to

---

[198] 47 U.S.C. § 230(c)(1).

[199] 47 U.S.C. § 230(c)(2)–(d).

[200] The Supreme Court struck down that provision in *Reno v. ACLU*, 521 U.S. 844, 885 (1997).

[201] 47 U.S.C. §§ 230(b)(3)–(4).

[202] 47 U.S.C. § 230(d).

children.[203] Congress was demonstrably mindful of those expressive torts in the text and legislative history and essentially silent about all others.

This narrower interpretation of the statute follows the traditional canon of construction that legislators do not "hide elephants in mouse holes."[204] Congress would surely have been far more explicit about a broader scope of protection had it meant to so radically reform the republication rule.[205] In any event, the narrower reading that I posit here would encourage the kind of sociability and altruism one would expect from a statutory provision that, in its title, explicitly seeks to protect Good Samaritans from liability for their good-faith efforts.

2. *How Much Creation and Development?*

We also do not know from the statute's plain terms or the legislative history what kind of activity constitutes "creation or development" under Section 230(f)(3), the statutory definition of "information content developer."[206] A website's design necessarily determines the way in which users express themselves, whether by video, photo, text, or mere click, for example. After all, as I explain above, the form of an online communication (say, a Facebook advertisement, a Medium post, a Tweet, or a YouTube clip) is contingent on the interactive computer service's design.[207] This is to say nothing of the far thornier question of whether, today, at a time when algorithmic prediction and machine learning determine most users' online experiences, interactive computer services that employ these techniques are "creat[ing] or develop[ing]" content within the meaning of Section 230(f).[208]

D. *Judicial Elaborations*

Courts have assumed the responsibility of determining whether and to what extent online intermediaries owe any affirmative duties to manage their users' content or conduct. Over the past two decades, they have read

---

[203] *See* Sherman v. Yahoo, 997 F. Supp. 2d 1129, 1137 (C.D. Cal. 2014) ("A plain reading of the statute indicates protection is intended only for the 'blocking and screening of offensive material.'").

[204] Whitman v. American Trucking Ass'n, 531 U.S. 457, 468 (2001) (citation omitted).

[205] *See* MCI v. AT&T, 512 U.S. 218, 228–29 (1994) (discussing narrow exceptions in Communications Act as evidence of the narrow meaning of the operative term). *See also* King v. Burwell, 135 S. Ct. 2480, 2495 (2015) (discussing Congress' tendency to avoid vague terms when altering regulatory schemes); Food & Drug Admin. v. Brown & Williamson, 529 U.S. 120, 160 (2000) (discussing Congress' tendency to avoid making changes to a regulatory scheme in a cryptic fashion).

[206] 47 U.S.C. § 230(f)(3) (2012).

[207] *See supra* Section B (discussing how application designs determine the form and substance of user content). *See, e.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003) (discussing matchmaker website's questionnaire and how it facilitated expression of information by individual users).

[208] *See supra* Part I.

the immunity under Section 230 broadly, despite the complications I suggest above.[209] First, they generally hold that the statute shields services from liability for all expressive torts by third parties, not just those that are reputational or harmful to children. Second, most courts have determined that the statute shields companies that do anything but elicit illegal or objectionable content from third parties by design. So, it is not enough that a service's administrators do not block or remove illegal content or, alternatively, solicit illicit material. Moderation of user content no longer seems to matter for the purposes of applying the immunity. Online intermediaries lose their immunity only if they have a hand in creating the illegal content or otherwise violate a separate duty that does not arise from the publishing event.[210]

This prevailing approach resonates with the longstanding skepticism in First Amendment doctrine of laws that have the effect of "chilling" conduct.[211] Of course, the subject and scope of protection in the constitutional setting are meaningfully different from those under Section 230. The constitutional provision establishes, among other things, a robust *ex ante* protection and affirmative defense from government "prior restraints" on speech.[212] Congress enacted the CDA, on the other hand, to shield private online companies from *ex post* private law claims for the misdeeds of private third-party actors.

But the "chilling effects" logic is nevertheless apropos. Without a broad immunity from liability, the theory goes, online entrepreneurs may not have as strong a native incentive to develop new applications or

---

[209] Jones v. Dirty World, 755 F.3d 398, 408 (6th Cir. 2014); Barnes v. Yahoo, 570 F.3d 1096, 1100 (9th Cir. 2009); Barrett v. Rosenthal, 146 P.3d 510, 523 (Cal. 2006); Zeran v. America Online, 129 F.3d 327, 332 (4th Cir. 1997).

[210] *See Jones*, 755 F.3d at 408 (discussing services losing immunity for being partly responsible for the creation or development of harmful content).

[211] *See, e.g.*, Miami Herald v. Tornillo, 418 U.S. 241, 257 (1974) ("Faced with the penalties that would accrue to any newspaper that published news or commentary arguably within the reach of the right-of-access statute, editors might well conclude that the safe course is to avoid controversy."); New York Times v. Sullivan, 376 U.S. 254, 266, 300 (1964) (applying chilling effects analysis to defamation claim arising from major news paper's publication of "matters of the highest public interest and concern"). According to one law review article, the term "chilling effect" first appeared in a Supreme Court opinion on a First Amendment controversy in *Gibson v. Florida Legis. Investigation Comm.*, 372 U.S. 539, 556–57 (1963). Frederick Schauer, *Fear, Risk, and the First Amendment: Unraveling the 'Chilling Effect,*, 58 B.U. L. REV. 685, 685 (1978); *see also* Ciolli, *supra* note 2, at 137, 148 (discussing the fear that over-censorship would hinder the open exchange of ideas on the internet); Kreimer, *supra* note 2, at 11, 47 (discussing the fear that censorship laws for online material could hinder free expression); Tushnet, *supra* note 2, at 986, 1013 (discussing the Court's efforts to balance the risk of harmful online speech with the risk of hindering the free exchange of information); Wu, *supra* note 2, at 293, 300 (2011) (discussing the fear that imposing excessive liability for distributing harmful speech will cause the censorship of too much content).

[212] *See* Near v. Minnesota, 283 U.S. 697, 716 (1931) (describing immunity from restraints or censorship as a long-standing liberty of the press).

services for fear of being sued.[213] Under the glare of litigious users, these deep-pocketed companies would have to bear the responsibility of monitoring their users' online behavior. The social costs of such an arrangement would be great. Service providers, whose interests do not necessarily align with those of their users, would censor their users for fear of being sued.[214] They, moreover, would have to divert resources to defend the parade of lawsuits arising from illegal third-party conduct. This would be a burdensome task for most online applications, but it would be especially onerous for companies like Reddit or YouTube that host massive amounts of third-party user content. Fewer users would likely join such services, diminishing the value of online engagement.

Empirically, it is hard to measure how innovative developers would be had Congress not enacted the CDA. The best we can do perhaps is compare online innovation in the U.S. with innovation in countries that do not have a similar immunity provision.[215] But even that would not reveal much because, by the mid to late 1990s, internet entrepreneurs in the U.S. had already obtained an advantageous (if not dominant) market position. In any event, U.S. courts have eagerly drawn on the chilling effects reasoning to articulate an extremely robust conception of Section 230 immunity.

This broad reading, however, was never inevitable. Courts in the Anglo-American common law tradition have long concluded that employers, hosts, and other intermediaries may be jointly, vicariously, or secondarily liable for illegal third-party conduct, despite the burden of having to attend to all conduct (expressive or otherwise) on their premises or by their employees or in their publications.[216] The reasons are obvious: intermediaries are often best able to curtail the costly effects of the underlying tort.[217] We might expect for the same reason that courts would not find it difficult to hold online intermediaries liable for hosting illegal

---

[213] *See* Tushnet, *supra* note 2, at 987 (discussing the challenge of "[c]reating incentives and obligations for intermediaries" without violating free expression principles).

[214] Wu, *supra* note 2, at 300.

[215] Europe's E-Commerce Directive, for example, establishes safe harbors for civil and criminal liability for third-party content. Directive 2000/31/EC of the European Parliament and of the Council on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. L 178/1. Those protections, however, are qualified by the nature of the intermediary and the underlying behavior. *Id.* at L 178/3, ¶¶ 12–14.

[216] *See* Colleen E. Medill, *The Federal Common Law of Vicarious Fiduciary Liability Under ERISA*, 44 U. MICH. J.L. REFORM 249, 254 (2011) (discussing the principal that a corporation is liable for the conduct of its agents while they act within the scope of their employment). *But see* Doe v. GTE Corp., 347 F.3d 655, 658 (7th Cir. 2003) (discussing the tendency of federal courts to refrain from creating broad secondary liability in the absence of a specified statute).

[217] *See* Guido Calabresi, *Some Thoughts on Risk Distribution and the Law of Torts*, 70 YALE L.J. 499, 500–01 (1961); *see also* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL L. REV. 1805 (2010).

third-party content or conduct. It would be fully consistent with a longstanding rule that such services owe duties because of their relative position in the political economy for distribution information.[218] Such a rule would not necessarily return us to *Prodigy* or the world before Section 230. Under this approach, immunity under Section 230 would only apply to cases in which plaintiffs allege that defendants were negligent in the efforts to take down such content.[219] And, today, with as much control as many providers have over their users' content by moderation and design, it would not be surprising for such a rule to take hold.

But the courts in the late 1990s chose a different path, even if sometimes begrudgingly.[220] The prevailing view was (and remains) that the social costs of policing online content would be too great to justify imposing liability on intermediaries for illegal third-party content.[221] Courts have found the old common-law tort view to be obsolete in the era of high-volume networked distribution of content, where the costs of policing bad actors are prohibitively expensive. They have read the immunity under Section 230 broadly, protecting service providers from liability for all third-party content to which they do not materially contribute. And this immunity is not contingent on good-faith efforts to moderate or take down objectionable content or making filtering technologies available to users. The guiding principle has been to ensure that users benefit from unfettered online speech and innovation.[222] The courts have concluded that reading the immunity broadly best achieves this end.

The courts' role here has been significant. In the absence of clarity from Congress, their broad reading of immunity likely accelerated the development of no-frills services like Craigslist and Reddit that seemed to do no more than host and publish user-generated content. By defining the immunity in the way that they did, the courts have been "technology-forcing,"[223] directing Silicon Valley to safely develop

---

[218] *See* Barnes v. Yahoo, 570 F.3d 1096, 1103 (9th Cir. 2009) (discussing *Hellar v. Bianco*, 244 P.2d 757, 758 (Cal. Ct. App. 1952)). It is ironic that the old common law rule imposed a duty on social hosts for the injuries caused by intoxicated guests to whom he or she has served liquor. Today, at least in some circles, to say that an online service "hosts" content is to suggest that it *does not* bear responsibility for the bad actions of its users. At least the etymology is intriguing.

[219] *See supra* Section II.D (discussing service providers hosting illegal content being held liable if they have a hand in creating it).

[220] *See, e.g.*, Blumenthal v. Drudge, 992 F. Supp. 44, 51–52 (D.D.C. 1998) ("If it were writing on a clean slate, this Court would agree with plaintiffs. . . . But Congress has made a different policy choice by providing immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others.").

[221] *Barnes*, 570 F.3d at 1099–1100.

[222] *Id.*

[223] *See* Motor Veh. Mfrs. Ass'n v. State Farm Ins., 463 U.S. 29, 49 (1983) (discussing the role of non-specific automobile safety standards in inducing the development of superior safety design).

intermediary "Web 2.0" services that do little more than host user-generated content. Of course, no matter how courts made sense of Section 230, their interpretations would have determined which sorts of applications would be winners and which would be losers in the Information Age. But there can be little question that, in the face of conflicting signals in the text and legislative history of the statute, the courts helped to determine the look and feel of the market during the crucial first decades after Congress enacted Section 230.

In the remaining Sections of this Part, below, I analyze how courts have come to this point. In the end, I show that, by reading the statute in the way that they have, courts have effectively turned the Good Samaritan purposes of the statute on its head. The doctrine now immunizes service providers who are antisocial as much if not more than those that moderate content.[224]

1. *The* Zeran *Framework*

The Fourth Circuit's 1997 opinion in *Zeran v. AOL* is easily the most-cited exemplar of the prevailing approach, even as the pertinent background facts in that case look relatively quaint in light of how existing online applications look and feel today.[225] There, an anonymous AOL user posted false advertisements for lewd merchandise that celebrated the 1995 Oklahoma City bombing on one of many America Online electronic bulletin boards. This user then directed interested subscribers to contact an unwitting user, plaintiff Zeran, at the latter's phone number. After receiving harassing calls and death threats, Zeran asked AOL to take the false advertisements down, which AOL did. But the anonymous originator continued to post new false advertisements over the next few days, requiring Zeran to contact AOL each time. AOL took the advertisement down each time, but also refused to abide by Zeran's request that the company issue a retraction or screen any future posts directed at him. Zeran accordingly sued a few months later, alleging several things, including that AOL, first, had a duty to take down all defamatory content as soon as it had notice of it, second, should have notified all AOL subscribers about the false nature of the advertisements, and, third, should have blocked all future defamatory statements about Zeran.

---

[224] David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 379–80 (2010); Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383, 389–90 (2009); *see also* Danielle Citron, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV. 1435, 1439 (2011) (discussing the freedom intermediaries have in choosing whether to challenge online speech).

[225] Zeran v. America Online, 129 F.3d 327, 332 (4th Cir. 1997).

The Fourth Circuit affirmed the trial court's decision to dismiss the claims. Section 230, it held, shielded AOL from liability. It did not matter that AOL had notice of the content. The statute, the panel explained, makes no distinction between a common law distributor and publisher.[226] Congress meant to protect both, as distributor liability is a subset of publisher liability.[227] Reciting the prefatory provisions of the statute, the court explained that the purpose of the statute was to keep government interference in the "burgeoning internet medium" to a minimum. Judicial remedies for expressive torts, it continued, would undercut the "diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity" that Congress explicitly enumerated in the findings on which the immunity is based.[228] The panel concluded, moreover, that Congress wrote the new statutory immunity to shield the likes of AOL from liability for the "millions" of expressive acts of third-party users that populate their service.

Ever since, federal and state courts across the country have modelled their analysis of immunity on the Fourth Circuit's.[229] This was especially true in the decade or so after Judge J. Harvie Wilkinson penned his opinion in *Zeran*, when the technology of online information distribution did not change much.[230] Defendant services generally invoked the immunity provision in disputes that began with a third-party user's reputationally injurious statements about another discrete user. The providers and users of an interactive computer service in these early cases simply relayed other users' online content. The specific third-party tortfeasor's expressive tort and the resultant injury on the plaintiff user were the bookends of the causal chain in these disputes.[231]

---

[226] *Id.*

[227] *Id.*

[228] *Id.* (citing 47 U.S.C. § 230(a)).

[229] *See, e.g.*, Green v. America Online, 318 F.3d 465, 471 (3d Cir. 2003); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1125 (9th Cir. 2003). This influence is probably an incident of the geography of internet entrepreneurship in the United States. AOL, the largest internet service at the end of the 1990s, was (and remains) headquartered in Northern Virginia, which is in the Fourth Circuit. The Ninth Circuit, in which Silicon Valley sits, would also play an outsized role in defining the doctrine.

[230] *See* ACLU v. Reno, 929 F. Supp. 824, 833 (E.D. Pa. 1996), *aff'd* 521 U.S. 844 (1997) (discussing origin of the internet and the prevailing way through which most users access it).

[231] Notably, this framework might also include the variety of other stakeholders who always play a constituent part in the transmission of information through and over the internet, including the broadband access providers for each respective user. Jones v. Dirty World Entm't Recordings LLC, 755 F.3d 398, 406 n.2 (6th Cir. 2014). But it does not necessarily include the long-haul network operators and administrators of internet traffic, or the domain registrar from which users get their domain names. This latter group, one way or another, contributes to the delivery of the content and better resembles conduits than online providers of "interactive computer service" because domain registrars generally deliver content without regard to its contents.

As antiquated as an electronic bulletin board may seem to social media users today, the main doctrinal issues have not changed much since *Zeran*. In many regards, the longevity of this approach suggests that the Fourth Circuit got it right twenty years ago. Today, courts first ask whether the service is a "publisher" of the offending material and, second, whether and to what extent the interactive computer service "creat[ed] or develop[ed]" the offending content.[232]

The courts settled on the core of the current doctrine in the mid to late 2000s. And, as I suggest above, they were likely motivated by the chilling effects line of argument as much as, if not more than, the plain text of Section 230(c). They have often parroted the statute's prefatory language to observe that burdening services with the actionable legal duty to monitor, block, and take down all illegal third-party material would discourage innovation and entrepreneurship. Congress, they have explained, wanted the "burgeoning Internet medium" to thrive, undeterred by the chilling threat of litigation.[233] A broad reading of immunity would best achieve these statutory purposes.[234]

---

[232] The question of whether the defendant "provider or user" is "responsible, in whole or in part," for the objectionable content under Section 230(f)(3) is important, but mostly derivative of the second question above about creation and development. *See* Fair Hous. Council of San Fernando Valley v. Roommates.Com, 521 F.3d 1157, 1171 (9th Cir. 2008) ("[E]ven if the data are supplied by third parties, a website operator may still contribute to the content's illegality and thus be liable as a developer . . . ."). The question of who is a "user" under Section 230(c)(1) was once unclear, but has since been resolved. The answer is: just about any entity, including natural persons, to whom a content developer "provides" the content for distribution. *See, e.g.*, Barrett v. Rosenthal, 146 P.3d 510, 522 (Cal. 2006) ("Congress implemented its intent not by maintaining the common law distinction between 'publishers' and 'distributors,' but by broadly shielding *all* providers from liability for 'publishing' information received from third parties."); Batzel v. Smith, 333 F.3d 1018, 1038 (9th Cir. 2003) ("Nothing in the text, legislative history, or human experience would lead me to accept the notion that Congress in § 230 intended to immunize users or providers of interactive computer services who, by their discretionary decisions to spread particular communications, cause trickles of defamation to swell into rivers of harm.").

[233] Zeran v. America Online, 129 F.3d 327, 330 (4th Cir. 1997).

[234] The courts' treatment of Section 230(d), an often-overlooked separate duty under the statute, also suggests that their reservations about imposing liability have likely not been particular to the text of the statute. Section 230(d), remember, requires providers of interactive computer services to notify new users, particularly parents of young children, about existing filtering software. Courts have said little to nothing about the provision and, to the extent they have said anything, they have not been inclined to enforce the obligation on providers that fail to inform their new users about filters. In 2013, for example, a Kentucky district court read Section 230(d) to mean that website operators would not receive immunity if they do not make attempts to screen third-party content and instead "invite invidious postings, elaborate on them with comments of their own, and call upon others to respond in kind." Jones v. Dirty World Entm't Recordings, LLC, 965 F. Supp. 2d 818, 822 (E.D. Ky. 2013), *rev'd* 755 F.3d 398 (6th Cir. 2014). The Sixth Circuit has rejected this "encouragement theory." *Id.* at 413–15 (reversing and vacating the district court's decision). In 2008, a federal district court in Utah found that a state law requiring internet service providers to provide filtering software (which they could do by "simply referring consumers to a third-party that provides filtering software when such software is requested") was not inconsistent with Section 230(d). Kings English, Inc. v. Shurtleff, No. 2:05-CV-

On the basis of this reasoning, in the decisive first several years after Congress enacted the statute, courts had no trouble shielding providers or users of interactive computer services from liability.[235] Companies like America Online were the clear beneficiaries in cases brought by individuals and companies for reputation-damaging third-party content.[236] In *Ben Ezra, Weinstein, and Company v. America Online*, for example, plaintiff sought monetary and injunctive relief for the web portal's publication of incorrect stock price and share volume information about plaintiff.[237] It alleged that AOL was liable for defamation and negligence because it had a hand in creating or developing the stock information and routinely revised or removed information about companies when it learned from the third-party stock information providers about errors.[238] The Tenth Circuit rejected plaintiff's claim, explaining that communications with the third-party content providers did not constitute development or creation under Section 230 and, in any case, by deleting incorrect information, AOL was "engaging in the editorial functions Congress sought to protect."[239] The court relied heavily on *Zeran* to support its conclusion.

The Section 230 defense also reached well beyond web portals like AOL in this early period. Smaller web-based providers and individual users also successfully claimed protection under the statute.[240] In *Batzel v. Smith*, an art collector brought defamation and related reputational injury claims against a relatively small website and listserv administrator for posting third-party allegations about her ownership of Nazi art.[241] In

---

485, 2008 U.S. Dist. LEXIS 60699, at *10–14 (D. Utah Aug. 8, 2008) (internal quotation marks omitted). Courts may have had little to say about that provision because Congress did not specify the sanction that courts may impose on providers that fail to adhere to its terms. And, yet, we might also assume that, had they been inclined to adopt a narrower conception of immunity that hewed more closely to the text of Section 230(c), they could have made immunity contingent on fulfilling the duty under Section 230(d).

[235] *See, e.g.*, Green v. America Online, 318 F.3d 465, 473 (3d Cir. 2003) (affirming the district court's finding that Section 230(c)(2) provided AOL with immunity for protecting its members from materials it considered objectionable to its subscribers); Ben Ezra, Weinstein, and Company v. America Online, 206 F.3d 980, 986 (10th Cir. 2000) ("Congress clearly enacted § 230 to forbid the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions."); Blumenthal v. Drudge, 992 F. Supp. 44, 50 (D.D.C. 1998) ("Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.").

[236] *See, e.g.*, *Green*, 318 F.3d at 473; *Ben Ezra*, 206 F.3d at 986; *Blumenthal*, 992 F. Supp at 50.

[237] *Ben Ezra*, 206 F.3d at 983.

[238] *Id.* at 983, 985.

[239] *Id.* at 986 (discussing *Zeran*).

[240] *See, e.g.*, Barrett v. Rosenthal, 146 P.3d 510, 520 (Cal. 2006) ("Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are barred."); Batzel v. Smith, 333 F.3d 1018, 1036 (9th Cir. 2003) ("[R]eject[ing] the argument that Mosler's continued sponsorship of the Network after Cremers published Smith's statements should give rise to liability.").

[241] See *infra* Section III.B.2 (discussing *Batzel*, 333 F.3d at 1018).

*Barrett v. Rosenthal*, a case decided by the California Supreme Court, doctors brought a defamation claim against the user of a consumer protection discussion group for impugning their character and competence.[242] The courts in both cases relied on Section 230 to dismiss plaintiffs' respective claims, explaining in both that the decision to post or not to post another user's content was an act of publishing within the meaning of the statute.[243] It did not matter that the defendants in each were users rather than providers of an interactive computer service.

The preponderance of these early cases involved discrete third-party posts of scandalous material about a discrete plaintiff user.[244] But many did not. Defendants invoked the immunity against claims for fraud and unjust enrichment,[245] business-related torts,[246] and breach of contract.[247] For the most part, however, the courts stayed true to the broad *Zeran* reading of Section 230 immunity. Their interpretation accordingly has facilitated the proliferation of online applications that depend on user-generated content: from social media to massively multiplayer online games to crowd-sourced review sites.[248]

2. *Material Contribution*

The cases that courts have been asked to resolve in recent years

---

[242] *Barrett*, 146 P.3d at 529.

[243] *Id.*; *Batzel*, 333 F.3d. at 1036. *But see* Maxfield v. Maxfield, No. FSTCV145014267, 2015 WL 9809777, at *3 (Conn. Super. Ct. Dec. 18, 2015) (finding that defendant is not "publisher or speaker" when retweeting defamatory material about ex-husband).

[244] *See generally* CTR. ON LAW AND INFO. POLICY AT FORDHAM LAW SCH., SECTION 230 OF THE COMMUNICATIONS DECENT ACT: A SURVEY OF THE LEGAL LITERATURE AND REFORM PROPOSALS (Apr. 25, 2012) (surveying sixteen years of Section 230 cases).

[245] *See, e.g.*, Ramey v. Darkside Prods., Inc., No. 02-730 (GK), 2004 WL 5550485, at *1 (D.D.C. May 17, 2004) (granting defendant's motion for summary judgment in case involving nude dancer's claims for fraud, intentional infliction of emotional distress, unjust enrichment, and negligence for using intimate photos on a pornography website without consent).

[246] *See, e.g.*, Mail Abuse Prevention Sys. LLC v. Black Ice Software, Inc., No. CV788630, 2000 WL 34016435, at *1 (Cal. Super. Ct. Oct. 13, 2000) (service provider claiming for, inter alia, intentional interference with contractual relationships, unfair competition, and restraint of trade for flagging plaintiffs' emails as spam).

[247] Schneider v. Amazon.com, Inc., 31 P.3d 37, 38–39 (Wash. App. Div. 1 2001) (author bringing breach of contract claim for failing to remove negative customer reviews of book).

[248] *See, e.g.*, Kimzey v. Yelp! Inc., 836 F.3d 1263, 1266 (9th Cir. 2016) (affirming district court's granting of Yelp!'s motion to dismiss given Congress' recognition that internet activity flourishes with minimal government regulation); Klayman v. Zuckerberg, 753 F.3d 1354, 1355 (D.C. Cir. 2014) (affirming district court's finding that the Communications Decency Act of 1996 shields Zuckerberg and Facebook from suit); Hill v. StubHub, Inc., 727 S.E.2d 550, 552 (N.C. App. 2012) (reversing trial court's decision and holding that online ticket reseller is immune from liability for allowing users to resell tickets in its online marketplace even if the user's actions violated the state's anti-scalping statute). *But see* Hassell v. Bird, 247 Cal. App. 4th 1336, 1341 (Cal. Ct. App. 2016), granting review, 381 P.3d 231 (2016) (affirming trial court injunction on non-party crowd sourced review site to remove negative reviews of plaintiff).

continue to present familiar fact-patterns involving discrete, reputation-damaging third-party statements.[249] But many arise from disputes that diverge from the *Zeran* framework. Indeed, by the mid-2000s, defendant providers were no longer simple conduits of the AOL variety. They were now designing social networking applications for dating and socializing as well as crowdsourced applications for knowledge production,[250] financing,[251] user reviews,[252] and traffic monitoring.[253] Section 230 doctrine likely helped to fuel this expansion. That is, while the drafters of Section 230 could not have anticipated these emergent applications or services, they surely heralded their possibility.

Entrepreneurs, in turn, raced to design and market lucrative services, free from the chilling threat of secondary liability. We can assume that there was very little that was malevolent in this ambition. The driving ethos for many of these entrepreneurs was to facilitate connections around the world.[254]

But the contours of the Section 230 doctrine would have to adapt. Courts would have to recalibrate the *Zeran* framework to attend to immersive and affecting applications that neither Congress nor the Fourth Circuit could anticipate. The specific question of how to gauge the extent of provider creation and development would become more complicated as developers designed applications that automated user-to-user interactions, effectively requiring courts to revise the way in which they conceived of the online "publisher or speaker" role.

One of the more instructive cases to take up the challenge was *Fair Housing Council of San Fernando Valley v. Roommates.com*.[255] That case concerned an ostensibly well-meaning, web-based service that matched people looking for a place to live with people offering rooms to rent.[256] The defendant's website consisted of two pertinent features that created a great opportunity for the Ninth Circuit to spell out how far courts would be willing to allow the immunity under Section 230 to reach.

---

[249] *See, e.g.*, Huon v. Denton, 841 F.3d 733, 741 (7th Cir. 2016).

[250] Wikipedia.com is an example of this.

[251] Artistshare.com, Indiegogo.com, and Kickstarter.com are examples of crowdsourced applications for financing.

[252] Yelp.com is such a website.

[253] Waze.com is an example of a crowdsourced application for traffic monitoring.

[254] *See* Mark Zuckerberg, *Is Connectivity a Human Right?*, https://scontent.fijd1-1.fna.fbcdn.net/v/t39.2365-6/12057105_1001874746531417_622371037_n.pdf?oh=ee304c17ab2509f1a5ba969786a8372e&oe=59EEE927 ("I'm focused on this because I believe it is one of the greatest challenges of our generation. The unfair economic reality is that those already on Facebook have way more money than the rest of the world combined, so it may not actually be profitable for us to serve the next few billion people for a very long time, if ever. But we believe everyone deserves to be connected.").

[255] 521 F.3d 1157 (9th Cir. 2008).

[256] Roommates.com still exists. But since the case, the website operates a little differently than it did ten years ago.

In order to subscribe to the service as either a room-hunter or offeror, Roommates required users to create a profile by choosing from a closed universe of biographical facts, including sex, sexual orientation, and whether the user has children.[257] The service similarly required prospective subscribers to convey which of these attributes—sex, sexual orientation, and having children—they prefer in roommates.[258] Roommates would use these preferences to classify, filter, and pair subscribers. Second, the service invited subscribers to provide "Additional Comments," without any direction about what those comments convey.[259] Users, as it turned out, used this space in their profile to express preferences about prospective roommates' gender, race, sexual orientation, and family status.

Plaintiff, a civil rights group, sued alleging that the Roommates service consisted of explicitly eliciting and communicating information about prospective renters and lessors in violation of federal and state fair housing law.[260] The federal FHA flatly bars real estate brokers from eliciting information about a prospective renter or buyer's sex, sexual orientation, or family status or indicating a preference for renters or buyers along any of those dimensions.[261] The fair housing advocates that brought the case argued that, by conditioning participation in the service on reporting restricted information, Roommates is an information content developer within the meaning of the statute, not a passive conduit.[262]

The Ninth Circuit, sitting en banc, agreed.[263] As alleged by plaintiff, Roommates' classifications, filtering, and matching functions, the panel concluded, were not immune from liability because Defendant steered subscribers based on attributes that are forbidden by federal and state fair housing laws.[264] To be sure, third-party subscribers selected among the listed preferences and, when they did so, were "[ ]other content developers" within the meaning of Section 230.[265] The court explains that this, however, did not preclude Roommates from being one as well.[266]

---

[257] *Roommates.Com*, 521 F.3d at 1161.

[258] *Id.*

[259] *Id.*

[260] *Id.* at 1162.

[261] 42 U.S.C. § 3604(c).

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

[263] *Id.* at 1165.

[264] *Id.* at 1169.

[265] *Id.* at 1165.

[266] *Id.* at 1165, 1167 ("[T]he party responsible for putting information online may be subject to liability, even if the information originated with a user. . . . At the same time, reading the exception for co-developers as applying only to content that originates entirely with the website . . . ignores the words 'development . . . in part' in the statutory passage 'creation *or development* in whole *or in part*.'" (citing *Batzel*, 333 F.3d at 1033 and quoting 47 U.S.C. § 230(f)(3))).

Indeed, these third-party room hunters would not have violated fair housing law but for Roommate.com's design.

The court was forgiving of the "Additional Comments" feature of the website. Roommates did not contribute any part of what third-party users posted. The "Additional Comments" feature, the court concluded, was precisely the sort of user-generated content that Congress sought to encourage with Section 230.[267] Imposing a duty on services like Roommates to police those comments would impose the very burden that Congress meant to avoid. In the end, the Ninth Circuit remanded the case back to the trial court to determine whether the drop-down menus that Roommates employed to elicit illegal information in fact violated federal and state housing laws.[268] The Ninth Circuit's analysis of the two markedly different features of the rooming service delimits how far service providers may go before losing immunity under the statute.

*Roommates* is today one of the most cited authorities for the material contribution standard under Section 230. This is chiefly because the court went beyond the *Zeran* framework in its immunity analysis. It did not confine itself to the question of whether the defendant provider developed objectionable content that originates with a discrete, reputation-damaging post by a third party.[269] The court in *Roommates* held that the immunity may apply in the absence of a discrete harm to plaintiff.[270]

Based on this approach, search engines are immune from liability when they index websites that make unauthorized ringtones available to users;[271] consumer advocacy websites are immune from liability for soliciting, advertising, and claiming exclusive copyright ownership of

---

[267] *Id.* at 1174.

[268] *Id.* at 1175. On remand, the district court found that Roommates.com did not violate fair housing laws. Fair Hous. Council of San Fernando Valley v. Roommates.Com, 666 F.3d 1216, 1219 (9th Cir. 2012).

[269] Some federal courts have entertained a less demanding "encouragement test." *See, e.g.*, Doe v. Sexsearch.com, 502 F. Supp. 2d 719, 727 (N.D. Ohio 2007), *aff'd on other grounds*, 551 F.3d 412, 420 (6th Cir. 2008) ("[The Court should ask] whether the claim is directed toward the defendant in its publishing, editorial, and/or screening capacities, and seeking to hold it 'liable for its publication of third-party content or harms flowing from the dissemination of that content.'"). But the prevailing rule requires plaintiffs to allege or prove that the defendant materially contributed the essential elements of the illicit content. Jones v. Dirty World, 755 F.3d 398, 410 (6th Cir. 2014). The Sixth Circuit has explained that the encouragement test would chill sites from entertaining user reviews or comments. *Id.* at 414–15. Congress, the Sixth Circuit explained, envisioned a far more "uninhibited, robust, and wide-open internet" than the encouragement rule would allow. *Id.* at 415.

[270] *Roommates.Com*, 521 F.3d at 1174.

[271] *See* Manchanda v. Google, Yahoo, and Microsoft Bing, 16 CV-3350, 2016 WL 6806250 at *2, *7 (S.D.N.Y. 2016) ("Manchanda has not shown that Defendants' allegedly injurious conduct here—namely, their aggregation and indexing of websites in their capacity as search engines—satisfies this high standard of outrageousness."); Goddard v. Google, Inc., 640 F. Supp. 2d 1193, 1199 (N.D. Cal. 2009) (finding Google's use of its AdWords program acceptable under the immunity principle).

negative reviews of attorneys;[272] and employers are immune for the defamatory statements that their employees post.[273] In all of these instances, the courts have employed a generous protection from liability that requires plaintiffs to establish that the defendant intermediary materially contributed to the creation or development of illegal or illicit material.

The *Roommates* opinion, however, also opened the door to liability for intermediary design. It held, after all, that immunity may be inapplicable when the defendant provider violates a law by virtue of its design, unrelated to whether plaintiff has experienced a discrete injury.[274] It was enough that the plaintiff civil rights organization stood in for the public to articulate the injury under the fair housing laws. We have yet to see how far this aspect of the holding will go. I will return to this below, in Parts III and IV.

Indeed, the protection under Section 230 remains robust. But all is not lost to plaintiffs. As protective of intermediaries as courts have been, they also have held that duties to users (and all others) remain if they do not arise from the "publishing" event, but rather from some separate or intervening condition.[275] So, an unfulfilled promise from Yahoo to take down defamatory third-party posts creates the duty to do so if the promisee relied on Yahoo's representations.[276] Model Mayhem, a company that administers an online marketplace for models to advertise themselves to agencies and advertising firms, is not immune from liability for failing to warn users about two men it knows have used its website to lure women to offline locations where the men sexually assault them.[277] Airbnb does not have a Section 230 defense and may be liable for failing to verify that hosts have registered with San Francisco as lessors of their short-term rental units.[278] A marketing network that places clients' advertisements on affiliated "fake news" sites was not immune for publishing the deceptive product information in the advertisements.[279] Google is not immune under

---

[272] *See* Small Justice LLC v. Xcentric Ventures LLC, 99 F. Supp. 3d 190, 200 (D. Mass. 2015) (finding Xcentric Ventures LLC's activities to be in accordance with the immunity principle).

[273] Davis v. Motiva Enterprises, L.L.C., No. 09-14-00434-CV, 2015 WL 1535694, at *1–2, *5 (Tex. App. Apr. 2, 2015), *appellate review denied* (June 19, 2015).

[274] *Roommates.Com*, 521 F.3d at 1174–75.

[275] *See, e.g.*, Doe v. Internet Brands, Inc., 824 F.3d 846, 853 (9th Cir. 2016) ("[T]he CDA does not provide a general immunity against all claims derived from third-party content."); Barnes v. Yahoo, 570 F.3d 1096, 1105 (9th Cir. 2009) (indicating that there are some actions that the statute does not shield from immunity); Airbnb v. City & County of San Francisco, 217 F. Supp. 3d 1066, 1075 (N.D. Cal. Nov. 8, 2016) ("Requirements that might have an incidental ripple effect on Internet postings are not barred under the CDA.").

[276] *Barnes*, 570 F.3d at 1105.

[277] *Internet Brands*, 824 F.3d at 853–54.

[278] *Airbnb*, 217 F. Supp. 3d at 1070, 1076.

[279] *Leadclick Media, LLC*, 838 F.3d at 168.

Section 230 from District of Columbia consumer protection statutory claims because it removed the video in violation of its own terms of service.[280]

There is nothing particularly remarkable in this nuance, however. The only notable take-away from this emergent line of cases is that courts appear to be becoming far more attentive to the way in which plaintiffs seek remedies for the "publishing" event. The broad scope of protection from liability for bad acts that originate with third-party users is unchanged.

### 3. *Whither the Good Samaritan*

Courts rarely if ever draw on the biblical parable for which Section 230(c) immunity is conspicuously named. This is not that surprising, since, alone, a statute's heading is generally not dispositive, particularly if courts believe that it conflicts with the gist of the statutory text.[281] Nor, moreover, are religion or religious teachings supposed to supplant the hard work of statutory interpretation in our constitutional democracy.[282] Yet, a statute's title or headers may be useful when the meaning of a statutory provision is not clear,[283] because they "supply cues" about the legislature's intentions.[284] Accordingly, I offer here a word about the biblical reference.

The main scriptural account starts with a man that has been robbed, beaten, and left for dead on the side of a major commercial road.[285] Two passersby, a priest and a Levite, walk by in turn.[286] They each see the victim on the verge of dying but do nothing to help, consistent with interpretations of religious law that forbid defiling a corpse and avoiding uncleanliness.[287] A third passerby, a Samaritan, tends to the man's wounds, carries him on his donkey to a nearby inn, and pays the innkeeper for every day that the victim stays to recover.[288]

On its plain terms, the parable is jarringly dissonant with life online today, where service providers host misogynist attacks on celebrities and mendaciously defamatory tweets from the President of the United States. But if the caption and language of Section 230(c)(2)(A) is to be taken

---

[280] Song Fi Inc. v. Google, Inc., 108 F. Supp. 3d 876, 884 (N.D. Cal. 2015).

[281] Yates v. United States, 135 S. Ct. 1074, 1083 (2015).

[282] *But see* Holy Trinity Church v. United States, 143 U.S. 457, 469–70 (1892).

[283] Almendarez-Torres v. United States, 523 U.S. 224, 233 (1998) ("'[T]he title of a statute and the heading of a section' are 'tools available for the resolution of a doubt' about the meaning of a statute." (quoting *Trainmen v. Baltimore & Ohio R. Co.*, 331 U.S. 519, 528–29 (1947))); *see also Yates*, 135 S. Ct. at 1083 ("While these headings are not commanding, they supply cues."); *Holy Trinity Church*, 143 U.S. at 463 ("[Light is thrown upon the statute by the language of the title.").

[284] *Yates*, 135 S. Ct. at 1083.

[285] *Luke* 10:25–37.

[286] *Id.*

[287] GEZA VERMES, THE AUTHENTIC GOSPEL OF JESUS 152–54 (2004).

[288] *Luke* 10:25–37.

seriously, Congress sought to entreat people to attend to vulnerable online users in spite of popular injunctions against doing so.[289]

It is beyond dispute that today's online intermediary immunity doctrine does not encourage providers or users of interactive computer services to follow in the footsteps of our biblical hero. Section 230 has been invoked successfully by extremely unsympathetic defendants.[290] In light of monitoring costs, moreover, service providers have every incentive to be agnostic about the harmful effects that their users' communications may have on others, including and especially the most vulnerable and disempowered.

Putting aside the interesting question of whether governments are or should be in the business of inspiring good works,[291] after two decades of litigation, the courts have developed an immunity doctrine that turns the statute's titular objective upside down. They have held that Section 230's reach is not confined to reputational harms or content that is harmful to children,[292] the only categories of conduct to which the statute refers. The consensus rule today is that Section 230(c) immunizes *all* providers from liability for *all* tortious third-party user content to the extent they do not materially contribute to its creation or development.

More to the point, the courts have held that the immunity is not contingent on monitoring or voluntarily taking good-faith steps to screen or take down illicit content as the statute suggests. If it were, the courts have explained, the doctrine would divert resources to policing content and away from the development of new services. Instead, some courts have explained that Section 230(c)(2)(A) provides an alternative protection for service providers who take good-faith steps voluntarily to screen or remove objectionable content.[293] That protection is distinct from the broader

---

[289] DOUGLAS A. HICKS & MARK VALERI, GLOBAL NEIGHBORS: CHRISTIAN FAITH AND MORAL OBLIGATION IN TODAY'S ECONOMY 31 (2008) (quoting Martin Luther King, Jr., *A Time to Break Silence*, *in* A TESTAMENT OF HOPE: THE ESSENTIAL WRITINGS AND SPEECHES OF MARTIN LUTHER KING, JR. 231 (James M. Washington ed., 1991)).

[290] *See, e.g.*, Jones v. Dirty World, 755 F.3d 398, 417 (6th Cir. 2014) (finding website that enables users to anonymously post comments, photographs, and videos immune from liability under Section 230); Doe v. Backpage.com, LLC, 817 F.3d 12, 16, 18, 24 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017) (finding website that provides online classified advertising immune under Section 230).

[291] Tax law presents this question quite directly.

[292] *But see* Sherman v. Yahoo! Inc., 997 F. Supp. 2d 1129, 1137–38 (S.D. Cal. 2014) ("[T]he Court concludes that the 'good samaritan' immunity is inapplicable where Yahoo! did not engage in any form of content analysis of the subject text to identify material that was offensive or harmful prior to the automatic sending of a notification message.").

[293] *See* Barnes v. Yahoo, 570 F.3d 1096, 1105 (9th Cir. 2009) (explaining that Section 230(c)(2) "provides an additional shield from liability" for services that take good step measures to remove or restrict access to objectionable content). *See, e.g.*, *Motiva Enterprises*, No. 09-14-00434-CV, 2015 WL 1535694 at *2 (explaining that Section 230(c)(2) shields defendant-employer from liability for good-faith efforts to restrict employee-users from posting defamatory material online); Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 850 (W.D. Tex. 2007), *aff'd*, 528 F.3d 413, 422 (5th Cir. 2008) (explaining that

protection under Section 230(c)(1), which covers all providers that act as a "publisher or speaker," as long as they do not have a hand in "creating or developing" the objectionable content.[294]

This is to say that courts do not read Section 230(c) as doing what its title purports. In a rich irony, the statute now protects the apathetic service provider as much as the do-gooder, which is to say there is no incentive in law to be a Good Samaritan service provider. To invoke the language of economics, the doctrine has introduced "moral hazard."[295]

As I suggest in Part II above,[296] this broad protection is not the most straightforward way of making sense of Section 230(c), particularly in light of the teachings of the parable on which the title is based. But, with only a few notable exceptions, the courts have been uninterested in the point. The *Zeran* panel, for example, did not identify which provision of Section 230—(c)(1) or (c)(2)(A)—it relied on to reach its conclusion. This is not to say that it did not consider alternative forms of the immunity. The court there recognized that Congress sought to encourage self-regulation, a purpose that speaks directly to Section 230(c)(2)(A), and not necessarily Section 230(c)(1). But the court did so without explicit reference to those provisions. And it also drew a different conclusion: that the best way to encourage self-regulation was to immunize providers that are slow or even indifferent to user injury. Even more, other courts have written out the distinction between active and passive users of "an interactive computer service" under the statute, effectively equating those services that "actively post or republish information" and those that remove or simply do not publish objectionable content.[297]

But there was another way. Read closely, Section 230(c)(2)(A), as specific and relatively conditional as it is, resembles an operative provision, where Section 230(c)(1) blankly speaks of how to "treat" "publisher[s] or speaker[s]," without specific mention of the circumstances

---

Section 230(c)(2) protects service provider from any claims "seek[ing] to hold MySpace liable for ineffective security measures and/or policies relating to age verification").

[294] *Barnes*, 570 F.3d at 1105, 1107.

[295] Mary Anne Franks, *Moral Hazard on Stilts*, LAW.COM (Nov. 10, 2017), https://www.law.com/therecorder/sites/therecorder/2017/11/10/moral-hazard-on-stilts-zerans-legacy/ ("[T]here is no evidence that broad immunity from liability has done anything more than encourage websites and ISPs to be increasingly reckless with regard to abusive and unlawful content on their platforms.")

[296] *See supra* Section II.C.2 (discussing what constitutes creation and development under Section 230(f)(3)).

[297] *See* Barrett v. Rosenthal, 146 P.3d 510, 527–28 ("A user who actively selects and posts material based on its content fits well within the traditional role of 'publisher.'"); Batzel v. Smith, 333 F.3d 1018, 1032 (9th Cir. 2003) ("The scope of the immunity cannot turn on whether the publisher approaches the selection process as one of inclusion or removal, as the difference is one of method or degree, not substance.").

under which such an entity may be immune from liability.[298] Read in this way, Section (c)(1) only delimits the category of covered "providers or users of an interactive computer service." Section 230(c)(2)(A), on the other hand, is not so sweeping. It, rather, declares the conditions under which courts may not hold a Good Samaritan service provider liable, effectively encouraging such providers to take good-faith actions voluntarily to screen objectionable content. This reading of Section 230(c) would only apply the immunity when safe harbor conditions under (c)(2)(A) are met in the way that the title of Section 230(c) and parts of the legislative history suggest.[299] The canon of interpretation that privileges specific provisions over general ones supports this common-sense approach.[300]

Some courts have acknowledged that this is a plausible reading, but nevertheless declined to abide by it.[301] Thus, today, the practical effect of the current doctrine is to dissuade services from helping to protect users from attack. There is now nothing to be gained under law for application developers to be Good Samaritans online.

## III. DESIGNS BEYOND IMMUNITY

I have shown above in Part II that, while courts have not completely foreclosed relief to plaintiffs, current doctrine substantially limits the parties from which they may recover. A plaintiff must establish that the defendant's service or application "materially contributes" to third-party users' volitional online conduct. In practice, the doctrine makes legal challenges to intermediaries' designs especially difficult to win.

Recent developments, however, suggest that the tide may be turning. Popular intermediaries today do not resemble the publishers that Congress envisioned when it enacted Section 230. As I explained in Part I above, the most popular intermediaries today engineer almost every aspect of users' online experience. Courts may in this regard no longer presume that the underlying injury originates with a third-party user's objectionable volitional act. They may come to recognize that service providers' design

---

[298] *Cf.* Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003) (explaining that there are multiple ways to read Section 230(c)(1)) (Easterbrook, J.).

[299] *Accord* Sherman v. Yahoo, 997 F. Supp. 2d 1129, 1137 (S.D. Cal. 2014).

[300] *See, e.g.*, Fourco Glass Co. v. Transmirra Products Corp., 353 U.S. 222, 228 (1957) (explaining that "[s]pecific terms [in a statute] prevail over general" terms in a conflicting statute); Dodson v. Potomac Mack Sales & Service, 400 S.E.2d 178, 181 (Va. 1991) (explaining that when general and specific terms conflict, the latter prevails).

[301] *GTE Corp.*, 347 F.3d at 660; *see also* Barnes v. Yahoo, 570 F.3d 1096, 1105 (9th Cir. 2009) ("[I]f section (c) did provide equal protection, then '[internet service providers] may be expected to take the do-nothing option and enjoy immunity' because 'precautions are costly.'" (citing *GTE Corp.*, 347 F.3d at 660)).

of the choice architecture precipitate illegal expressive acts. The *Roommates* formulation in particular opens up the possibility that courts will attend to the design conditions under which illicit conduct may occur.

### A. *Structuring User Content*

As I explained above, *Roommates* is the leading case on the material contribution standard. But the Ninth Circuit's opinion there also sheds light on whether and how a developer's application design might be so affecting or assertive as to count as "development" under Section 230. The en banc court there held that Roommates could not be immune for illegal third-party content that it elicited.[302] Its designers structured the Roommates website to require subscribers to express preferences for gender, sexual orientation, and family size in violation of fair housing laws.[303] Users had no hand in selecting those listed items.[304] They had to choose among those options in order to subscribe.[305] The Ninth Circuit held that this feature of the website implicated Roommates in FHA violations every time someone used it to find a roommate.[306] The court held that the open "Additional Comments" online form, on the other hand, did not consign user responses in the same way and, therefore, did not implicate Roommates in the development of third-party user content.[307]

The Ninth Circuit's analysis in *Roommates* relied heavily on *Carafano*, decided five years before. That older opinion helps to explain the "material contribution" test and elaborates the later opinion's application to intermediary design.[308] There, an anonymous user created a false profile of the plaintiff on Matchmaker.com, a dating site operated by Metrosplash. Matchmaker required its participating members to reveal personal information through a questionnaire that contained over 50 multiple-choice questions and several open-ended questions.[309] The multiple-choice questions asked for such things as users' respective age, physical characteristics, interests, personality, and reasons for joining the service.[310] The open-ended questions invited users to submit whatever information or photos they thought were relevant to finding a mate, as long as it did not include risqué images or personally identifiable information like last name,

---

[302] Fair Hous. Council of San Fernando Valley v. Roommates.Com, 521 F.3d 1157, 1172, 1175 (9th Cir. 2008).

[303] *Id.* at 1161.

[304] *Id.* at 1166.

[305] *Id.*

[306] *Id.*

[307] *Id.* at 1173–74.

[308] *Id.* at 1171–72.

[309] Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1121 (9th Cir. 2003).

[310] *Id.*

home or email address, or phone number.[311] Matchmaker did not review each profile to ensure compliance.[312]

As in *Zeran*, nothing on the Matchmaker site could altogether bar anonymous users from impersonating someone else. That is how, in *Carafano*, an anonymous user based in Berlin created a false profile of the plaintiff, a relatively well-known California-based movie and television actress.[313] While he did not identify Carafano by her real or stage name, he still managed to suggest her identity by posting publicly available pictures and identifying two popular movies in which she was featured.[314] His answers to the multiple-choice questions were sexually descriptive and aggressive.[315] He also included an email address through which he set up an automatic reply that identified Carafano's real home address and phone number.[316]

Within days, Carafano was receiving phone calls, voice messages, email, mail, and faxes.[317] Several of the people who contacted her expressed concern that she might post such a profile online.[318] Most others, however, expressed genuine interest in meeting.[319] A few other messages were sexually explicit.[320] And a handful threatened physical harm to Carafano and her son.[321] The Matchmaker administrators deleted the false profiles days after Carafano's publicist contacted them.[322] But, of course, the damage had already been done. Carafano soon sued against Metrosplash, alleging invasion of privacy, misappropriation of the right of publicity, defamation, and negligence.[323]

The Ninth Circuit held that Matchmaker could not be held liable for the false Carafano profile because, even if the questionnaire elicited some of the illegal content, the anonymous third-party user, not Matchmaker, provided the "essential published content."[324] It did not matter, the court explained, that Matchmaker "facilitated the expression of information" or engaged in "specific editing or selection" in defining discrete categories or

---

[311] *Id.*
[312] *Id.*
[313] *Id.*
[314] *Id.*
[315] *Id.*
[316] *Id.*
[317] *Id.* at 1121–22.
[318] *Id.* at 1122.
[319] *Id.*
[320] *Id.* at 1121.
[321] *Id.*
[322] *Id.* at 1122.
[323] *Id.*
[324] *Id.* at 1124.

sorting users' answers.[325] "[T]he selection of the content was left exclusively to the user."[326]

The Ninth Circuit did not explain what it meant by "essential," but, as used there, the court foreshadowed the material contribution standard that it would later announce in *Roommates*. In *Carafano*, the panel acknowledged that the Matchmaker service made the illegal communication possible but, at the same time, determined that the company did not have a legally significant role in developing its "essential" elements. "Matchmaker cannot be considered an 'information content provider' under the statute," the panel explained, because the service only "structure[d] the information provided by users" in order to match them.[327]

The *Roommates* court relied heavily on its holding in *Carafano*. In that earlier case, the en banc Ninth Circuit explained, the content at issue was "created and developed entirely by the malevolent user, without prompting or help from the website operator."[328] In *Roommates*, however, the company developed "the discriminatory questions, discriminatory answers, and discriminatory search mechanism" before any new subscribers even expressed their preferences.[329] Roommates, moreover, "ma[de] aggressive use" of the content that it elicits from users "in conducting its business."[330]

The difference between contributions for which an intermediary may be liable and those for which it may not turns on how "essential" the intermediary is to the development of the illegal online conduct.[331] The immunity under this framing is not contingent on whether a third party provides the content. Nor does it depend on whether the provider's contribution is additive. After *Roommates*, the immunity may turn on the way in which the intermediary structures its service or application to receive and uses third-party material. This approach takes seriously the statute's assertion that service providers lose their immunity if they are "responsible, in whole or in part, for the creation or development of information."[332]

---

[325] *Id.* at 1124–25.

[326] *Id.* at 1124.

[327] *Id.* at 1124–25.

[328] Fair Hous. Council of San Fernando Valley v. Roommates.Com, 521 F.3d 1157, 1171 (9th Cir. 2008).

[329] *Id.* at 1172.

[330] *Id.*

[331] *Carafano*, 339 F.3d at 1124.

[332] 47 U.S.C. § 230(f)(3).

## B. *Design as Knowledge*

Missing from the discussion here (and the doctrine) has been any serious consideration of how much a defendant provider must know about the likelihood of harm to lose the immunity. We might understand the *Roommates* opinion to suggest that a provider cannot be immune when it has *knowingly* designed its service or application in order to elicit illegal third-party content. After all, Roommates deliberately designed its site so that all of its users had to choose between its prepopulated drop-down menu options.[333] As with most website developers, the company was probably very attentive to the substantive preference options from which it allowed users to choose, as well as the way it presented the choices for selection (i.e., choice architecture).

But the *Roommates* court did not frame its opinion in this way. Nor did it have to. After *Zeran*, subjective provider knowledge of user wrongdoing has no part in the current doctrine.[334] Two other cases help to explain: *Doe v. Myspace* and *Batzel v. Smith.*

### 1. *Subjective Knowledge about the Likelihood of Harm to Plaintiff*

In *Doe v. MySpace*, the defendant provider operated (and still operates) a social networking site that requires users to create profiles with a name, an email address, gender, country, and date of birth.[335] Users may also post photographs, videos, and any other information that they want to share with the public or, if they prefer, their circle of MySpace friends.[336] Users who were over age sixteen could limit which aspects of their profile could be seen by others.[337] MySpace, however, automatically rendered the profiles of users who are under sixteen private.[338] The service also developed software to ferret out teenagers who claimed to be older than they were, but this feature was far from foolproof since about 22 percent of its users were minors, and a large percentage of these users claimed to be older than they really were.[339]

Like many of her peers, Julie falsely represented that she was eighteen years old when she created her MySpace profile.[340] And she chose not to

---

[333] That Roommates did not include racial categories among its prepopulated drop-down menu suggests an unstated recognition on this point. It may be that they thought that such categories would be illegal, if not simply alarming.

[334] *See* Zeran v. America Online, 129 F.3d 327, 332 (4th Cir. 1997) ("[T]his theory of liability is merely a subset, or a species, of publisher liability, and is therefore foreclosed . . . .").

[335] Doe v. MySpace, 528 F.3d 413, 416–17 (5th Cir. 2008).

[336] *Id.* at 415.

[337] *Id.*

[338] *Id.*

[339] *Id.* at 416–17 (5th Cir. 2008).

[340] *Id.* at 416.

block access to her information.[341] Her personal information was therefore viewable by all MySpace users. It was under these conditions that Julie and a nineteen-year old man exchanged contact information.[342] The two eventually met in person and, there, at their first encounter, the older man sexually assaulted her.[343] Soon after, Julie and her mother brought a handful of tort claims against MySpace, including claims for negligence and gross negligence for failing to implement basic safety measures to protect minors from predators.[344] They argued that the physical sexual assault arose out of the connection Julie made by virtue of MySpace's questionnaire. The Does argued that the immunity provisions were inapplicable because MySpace was "partially responsible for creating the content" that brought Julie, a minor, in contact with her attacker.[345]

The Court of Appeals for the Fifth Circuit affirmed the trial court's dismissal of the Doe's claims.[346] The plaintiffs, the panel explained, were suing MySpace for publishing information for which Julie was wholly responsible.[347] She had done so in spite of MySpace's rule against such misrepresentations. Imposing liability on MySpace for the distribution of this content, the panel determined, was exactly what Congress wanted to block.[348]

MySpace's design was in no small part born from the broad interpretation of Section 230 immunity that the courts had developed in the decade before. The company curated the information that users shared with others. And it did so knowing that over a fifth of its users were minors and that many of these, in turn, misrepresented their age. This is to say that the company actively courted children, knowing that many of them would misrepresent their age.

One might assume that a statute addressed to protecting children from objectionable online content would not immunize websites that knowingly expose children to danger. But, for the Fifth Circuit, that consideration hardly made an appearance in the opinion. For the panel, plaintiffs had to be far more engaged in the underlying tort—perhaps by explicitly eliciting an incorrect age or encouraging a sexual encounter between underage Julie and her adult assailant.[349] Without such allegations, the court determined

---

[341] *Id.*

[342] *Id.*

[343] *Id.*

[344] *Id.* at 416.

[345] *Id.* at 417.

[346] *Id.* at 415.

[347] *Id.* at 421.

[348] *See id.* at 419 ("Congress made a policy choice, however, not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages.").

[349] *Id.* at 420.

that MySpace owed no obligation to implement any further safety measures to bar minors from interacting with adults, even as it knew that a meaningful number of the children who used the application were vulnerable.

This approach is quite unlike the way in which courts analyze the scope of liability in cases involving claims that a defendant intermediary has generalizable or specific subjective knowledge that its service or product facilitates copyright violations.[350] Pursuant to the Digital Millennium Copyright Act, the 1998 amendment to the Copyright Act, a provider is obliged to remove infringing material when it has "actual knowledge" of it on its site or is "aware of facts or circumstances from which infringing activity is apparent."[351] Under Section 230, on the other hand, services like MySpace are shielded from liability for publishing users' information even though its administrators understood with a relatively high degree of confidence that minors were misrepresenting their ages on the site and that, by doing so, those children were making themselves vulnerable to attack. The company's policy of automatically protecting the privacy of users under the age of sixteen betrays its knowledge of the risks. But its awareness of wrongdoing was not salient enough to sway the court against MySpace. For the panel, the social media company owed no duty to attend to patterns of deception (on the part of children) and abuse (on the part of adults), no matter how pernicious or predictable.

There is at least one sliver of hope for plaintiffs set on premising their theory of service provider liability on the provider's subjective knowledge of third-party wrongdoing. One year after the decision in *Roommates*, in *Federal Trade Commission v. Accusearch*, the Tenth Circuit suggested that a defendant-provider's knowledge may indeed be important to understanding the materiality of its contribution to illegal third-party

---

[350] *See* Metro-Goldwyn-Mayer Studios v. Grokster, 545 U.S. 913, 933–34 (2005) ("The Ninth Circuit has read Sony's limitation to mean that whenever a product is capable of substantial lawful use, the producer can never be held contributory liable for third parties' infringing use of it; it read the rule as being this broad, even when an actual purpose to cause infringing use is shown by evidence independent of design and distribution of the product, unless the distributors had specific knowledge of infringement at a time at which they contributed to the infringement, and failed to act upon that information."); Sony Corp. of America v. Universal City Studios, 464 U.S. 417, 487 (1984) ("Moreover, a finding of contributory infringement has never depended on actual knowledge of particular instances of infringement; it is sufficient that the defendant have reason to know that infringement is taking place."); Viacom Int'l v. YouTube, 676 F.3d 19, 30 (2d Cir. 2012) ("In light of our holding that § 512(c)(1)(B) does not include a specific knowledge requirement, we think it prudent to remand to the District Court to consider in the first instance whether the plaintiffs have adduced sufficient evidence to allow a reasonable jury to conclude that YouTube had the right and ability to control the infringing activity and received a financial benefit directly attributable to that activity.").

[351] 17 U.S.C. § 512(c) (2010).

content.[352] Importantly, there, the defendant's knowledge was evidenced by the systems it put in place to generate third-party content. In this case, the defendant operated a website that sold personal information about individuals, including telephone records.[353] Users of Accusearch's service paid an "administrative search fee" to obtain public and private information about people.[354] The company, in turn, contracted with third-party researchers to retrieve the sought information "in accordance with applicable law."[355] Once retrieved and formatted, Accusearch delivered the information to the requesting customer's online account.[356] The Federal Trade Commission sued, alleging, among other things, that Accusearch committed an unfair trade practice under the Federal Trade Commission Act whenever it obtained and made confidential customer telephone records publicly available.[357] Accusearch moved for summary judgment on Section 230 grounds.[358]

The question for the Tenth Circuit panel was whether Accusearch created or developed the confidential telephone information under Section 230(f)(3) by engaging researchers to retrieve it.[359] The court answered that Accusearch did and, therefore, was ineligible for immunity.[360] The term "development," it explained, should be read to encompass "the act of drawing something out, making it visible, active, or usable."[361] The term "responsible" under Section 230, it continued, suggests that the provider is

---

[352] *See* FTC v. Accusearch, 570 F.3d 1187, 1199 (10th Cir. 2009) ("Accusearch solicited requests for such confidential information and then paid researchers to obtain it. It knowingly sought to transform virtually unknown information into a publicly available commodity. And as the district court found and the record shows, Accusearch knew that its researchers were obtaining the information through fraud or other illegality.").

[353] *Id.* at 1190.

[354] *Id.* at 1191.

[355] *Id.*

[356] *Id.*

[357] *See id.* at 1192 (alleging that Accusearch's conduct violated the FTC Act to the extent 47 U.S.C. § 222 makes consumer telephone records confidential).

[358] *Id.* at 1192–93.

[359] *Id.* at 1198; *see also* Blumenthal v. Drudge, 992 F. Supp. 44, 50 (D.D.C. 1998) ("While Section 230 does not preclude joint liability for the joint development of content, AOL maintains that there simply is no evidence here that AOL had any role in creating or developing any of the information in the Drudge Report. The Court agrees."). The panel dispensed with the question of whether Accusearch was a publisher within the meaning of the statute in very short order. *Accusearch*, 570 F. 3d at 1197. The concurring opinion was of the view that plaintiff was not challenging the defendant for publishing, but for its "unfair" conduct. *See id.* at 1206 (Tymkovich, J., concurring) ("Accusearch's duty to refrain from engaging in these unfair business practices does not derive from its status or conduct as an Internet website that publishes content.").

[360] *Accusearch*, 570 F. 3d at 1198.

[361] *Id.* (quoting *Develop*, WEBSTER'S NEW INTERNATIONAL DICTIONARY (3d ed. 2002)) (internal quotations marks omitted).

"more than a neutral conduit for . . . content."[362] Section 230 would not allow courts to impose liability on a service provider in the same way that a highway builder could not be responsible for a banker's escape.[363] Thus, under the statute, the panel concluded, "a service provider is responsible for the development of offensive content only if it in some way specifically encourages development of what is offensive about the content."[364]

This, the Tenth Circuit concluded, is what Accusearch did when it routinely contracted with third-party researchers to retrieve customer information it knew to be illegal. Unlike *Ben Ezra*, where defendant AOL solicited information that happened to be inaccurate, Accusearch *knowingly* sought to obtain confidential consumer information in order to share it with the public.[365] Accusearch's solicitation and collection of private customer information, the court observed, was its reason for being.[366]

This, recall, was similar to Roommates' failing. The real estate search service there required third-party users to provide illegal responses to illegal questions in order to participate. Connecting users based on the restricted demographic information that Roommates elicited and sorted was the application's reason for being. To be sure, the (restricted) dimensions on which Roommates relied to facilitate reliably strong matches were salient. But that is precisely why Congress forbade their consideration. The Ninth Circuit held that, no matter how valuable information about a prospective roommate's gender or sexual orientation might be, it is illegal to traffic in it when looking for a roommate.[367] Eliciting that information harms disfavored groups in exactly the ways the fair housing laws forbid.

In this way, it may be that the potential violation in *Roommates* was far worse than that in *Accusearch*, because, unlike the latter, *every* third-party response in the former was illegal. And, more to the point here, Roommates designed its application in order to collect and publish the illegal information. To the extent Accusearch was implicated in the development of illegal content, it was because the company paid

---

[362] *Id.* at 1199 (quoting *Responsible*, WEBSTER'S NEW INTERNATIONAL DICTIONARY (3d ed. 2002)) (internal quotations marks omitted).

[363] *Id.* at 1199.

[364] *Id.* (internal quotations omitted). In its phrasing, the panel here suggested that it may have employed the "encouragement" test that most courts have rejected. The *Accusearch* panel, however, explicitly adhered to the prevailing material contribution standard in other parts of the decision.

[365] *See id.* at 1199. ("Accusearch *knew* that its researchers were obtaining the information through fraud or other illegality." (emphasis added)).

[366] *See id.* at 1200 ("[T]he offensive postings were Accusearch's raison d'etre . . . .").

[367] *See* Fair Hous. Council of San Fernando Valley v. Roommates.Com, 521 F.3d 1157, 1174 (9th Cir. 2008) (absolving Roommates from liability because it is not responsible for the content being created by its users).

researchers to obtain information it knew to be illegal.[368] But those violations occurred only when a subscriber sought that kind of personal information.[369]

2. *Objective Knowledge about Third-Party User Intent*

This is not to say that courts do not consider a service provider's knowledge of wrongdoing to determine the applicability of Section 230 immunity. The Ninth Circuit did in at least one case early in the statute's life. In *Batzel v. Smith*, the Ninth Circuit held that a defendant provider's knowledge was pertinent to determining whether the third party "provided" the content at issue for publication. "Publishing," it held, could only occur if the provider reasonably believes that it was the third-party user's intention to have the material published.[370] The opposite rule, the court explained, would confer "nearly limitless immunity for speech never meant to be broadcast over the Internet,"[371] and accordingly work against Section 230's objective to encourage providers "to remove offensive material."[372] To shield the defendant in that case from liability, the panel observed, would have the opposite effect; it would protect providers who attribute objectionable content to unwitting third parties.[373]

The third party in that case, Robert Smith, was a building contractor who had reason to believe that one of his clients, plaintiff Ellen Batzel, inherited paintings that had been illegally stolen by the Nazis in the years before World War II.[374] Smith sent an email message that conveyed his suspicions to an email address that he found online for the Museum Security Network, an online network devoted the retrieval of stolen art.[375] The recipient of the email, Ton Cremers, immediately forwarded Smith's

---

[368] *Id.* at 1199.

[369] A very recent case, *FTC v. LeadClick Media*, 838 F.3d 158 (2d Cir. 2016), falls somewhere between *Roommates* and *Accusearch* on the dimension of pertinent provider knowledge. LeadClick operated a marketing network that placed client-merchants' advertisements on affiliated "fake news" sites. Most if not all of the clients with which the company did business marketed popular weight-loss products. It administered this line of business through software that innocuously tracked and monetized user traffic from the affiliated site to the merchant's site. *Id.* at 163–64. LeadClick's eight to ten employees cultivated relationships with these affiliated fake news sites and, in some cases, even directed and edited content about the efficacy of the products. These affiliated sites falsely claimed that, pursuant to testing, the weight loss product showed appreciable effects on consumers. *See Accusearch*, 570 F.3d at 1200 ("By paying its researchers to acquire telephone records, knowing that the confidentiality of the records was protected by law, it contributed mightily to the unlawful conduct of its researchers.").

[370] Batzel v. Smith, 333 F.3d 1018, 1034 (9th Cir. 2003).

[371] *Id.* at 1033. Even in 2003, courts were mixing metaphors associated with different media technologies.

[372] *Id.* at 1034.

[373] *Id.* at 1034.

[374] *Id.* at 1021.

[375] *Id.* at 1021.

email to the Network's affiliated listserv and also posted it on the website after making minor edits.[376] Trial discovery suggested that Smith did not know that his email would be forwarded to the Network's international email address list.[377]

Her reputation tarnished, plaintiff sued Smith, Cremers, and others for defamation.[378] She argued that she was not related to Nazis and that the art was not looted Nazi art.[379] Cremers answered that, among other things, he could not be held liable for posting Smiths' defamatory statements on the website because he is a publisher that "did no more than select and make minor alterations to Smith's email."[380]

The panel sided with Cremers.[381] And, in this regard, *Batzel* ratified the emergent view then in 2003 that providers of interactive computer services would find a generous protection under Section 230(c) to publish illegal third-party content without concern about liability.[382] But, far more pertinently, the Ninth Circuit remanded the case to the trial court for more fact-finding on whether a reasonable provider could believe that Smith intended to the have the contents of his email message forwarded or published to the Network's listserv.[383] This is to say that the court did not remand the case to the district court to inquire into Cremers' subjective impressions of Smith's intentions. Section 230 makes no provision for that kind of consideration. Nor was the lower court to concern itself with whether Cremers meant to do harm by publishing the contents of Smith's email. The panel's opinion disposed of that question. Rather, the Ninth Circuit charged the trial court with the task of determining whether, objectively, a provider or user of an interactive computer service could reasonably believe that Smith wanted him to publish the contents of the email.

Since *Batzel*, courts do not bother to inquire into providers' subjective knowledge of or intention to publish illegal content. Nor, after *MySpace*, does the doctrine consider intermediaries' knowledge of the likelihood of wrongdoing pertinent to the immunity analysis. The doctrine is simply not concerned with providers' subjective intentions, in spite of the language in Section 230(c)(2) addressed to "good faith."

The *Batzel* panel, however, did think it important to recognize that intermediaries are obliged to heed the intentions of third-party users. At a

---

[376] *Id.* at 1022.
[377] *Id.*
[378] *Id.*
[379] *Id.*
[380] *Id.* at 1031.
[381] *Id.*
[382] *Id.*
[383] *Id.* at 1035.

minimum, this elaboration allows that an intermediary may be liable if it is unreasonable in its assessment of whether a third-party user sought to publish content. Sometimes circumstances surrounding providers' acquisition of third-party content are sufficiently unclear as to counsel against immunity for publishing that content. This is a far cry from the kind of subjective knowledge that courts consider in cases involving publishing torts in other settings.[384] But, in any event, this elaboration in the doctrine offers something of an opening into provider decision-making processes. It requires that intermediaries be reasonable in their editorial decision to publish third-party content. They may not veer away from or be inattentive to the expectations of their users. This elaboration could have purchase in an online information ecosystem in which users share information to providers that is later used by that provider in some ancillary or unrelated secondary market. I turn to this point in the next and final Part of the Article.

## IV. DESIGN DUTIES: REIMAGINING IMMUNITY

### A. *Designs on Ancillary or Secondary Markets*

Courts have interpreted Section 230 broadly. They do not consider the voluntary good-faith efforts of defendant providers, in spite of the evocative Good Samaritan language in the statute. Nor do they inquire into providers' subjective knowledge or control of third-party wrongdoing, as they do under traditional intermediary-liability rules.[385] Courts today are reluctant to impose liability on online intermediaries in the name of preserving the generative ethos of openness and innovation.

This laissez-faire approach made sense in the late 1990s and early 2000s, when service providers offered themselves as little more than the conduits through which content flowed between users. Today, however, the most popular intermediaries only "publish" a fraction of the information that users "provide" in the way that those users intended. Intermediaries instead collect, analyze, collate, and reconfigure the content for markets from which those original users gain no material direct benefit.

---

[384] *See, e.g.*, Viacom Int'l v. YouTube, 679 F.3d 19 (2d Cir. 2012).

[385] *Compare* 17 U.S.C. § 512(c), Metro-Goldwyn-Mayer v. Grokster, 545 U.S. 913, 937 (2005) ("Mere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability."), *and* Sony v. Universal City Studios, 464 U.S. 417, 439 (1984) ("If vicarious liability is to be imposed on Sony in this case, it must rest on the fact that it has sold equipment with constructive knowledge of the fact that its customers may use that equipment to make unauthorized copies of copyrighted material."), *with* Viacom v. YouTube, 676 F.3d 19, 41 (2d Cir. 2012) ("The District Court correctly held that 17 U.S.C. § 512(c)(1)(A) requires knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement . . . .").

This must complicate the immunity analysis because the practice of trading in user data—that is, after the analysis and sorting—does not fit easily within the scope of Section 230. First, the behind-the-scenes "block box" algorithmic processing on which intermediaries depend ostensibly produces new content that they then make available to other parties in ancillary and secondary markets. Providers like these do not resemble the traditional conduits envisioned by the framers of Section 230. Nor do the ways in which these intermediaries later make user data available in ancillary or secondary markets look anything like the publishing events envisioned in the doctrine. Nor, of course, do they involve the communication of "objectionable" "material" as was meant by Congress in 1996.

To the extent there is anything troubling in the administration of users' content on social media and online marketplaces, it is in the way in which providers "publish" or, rather, repurpose and exploit users' content. And the current Section 230 doctrine does not allow courts to account for it.[386] As I have shown here, however, application designs implicate intermediaries in the creation and development of user content in each instance. Some applications, like Reddit and Twitter, for example, allow their users to use pseudonyms. This has the effect of instilling in users a sense that no issue or topic, no matter how unlawful or objectionable, is taboo. Others, like Amazon or Tinder, are more engaged, acting as online concierges and curators; they make recommendations about products and potential partners based on each users' idiosyncratic interests and desires. And still others, like Netflix or Facebook, sort and monetize their users' data in ancillary or secondary markets. Indeed, intermediaries in this third category are involved in a two-sided business: one that collects user information by dint of their ostensible role as a conduit of communication and another that markets user data to advertising networks and data brokers.[387] A final fourth category of intermediaries surreptitiously designs their applications with the purpose of directing user behavior. Consider the admittedly extreme example of Uber, the ride-hailing smartphone app, that has surreptitiously employed a variety of deceptive techniques to manipulate drivers and dupe regulators.[388]

---

[386] *See supra* Part I (explaining 47 U.S.C. § 230).

[387] *See* NICK SRNICEK, PLATFORM CAPITALISM (2016); *see also* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. (forthcoming 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2935321 ("Surveillance intermediaries also sometimes enable the government's surveillance capabilities, whether by serving as 'fourth-party' data brokers that purchase, package and resell user data, or by providing infrastructure and technology . . . .").

[388] *See* Mike Isaac, *Uber's C.E.O. Plays with Fire*, N.Y. TIMES (Apr. 23, 2017), https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html (discussing how Uber added a "de Blasio" tab in its app to show lengthy wait times when Mayor Bill de Blasio attempted to limit the number of Uber cars); Noam Sheiber, *How Uber*

It is clear then that, today, the information that users share does not necessarily flow untouched through providers' servers, from user to user. And it is not "published" in the way Section 230 contemplates. The manner in which applications marshal user information varies greatly. The most commercially successful online companies today design their services to collect as much user information as possible. They elicit, structure, sort, and sometimes market and sell the user data they receive. Mindful of its value, moreover, these intermediaries employ clever techniques that keep users coming back to give more.[389] In this way, application developers may be far more involved in generating user content and online behavior than the *Zeran* framework contemplates. At best, these services only pretend to be passive platforms that facilitate user interactions.

Many, if not most intermediaries today are more implicated than courts believed them to be just a decade ago. In *Roommates*, the defendant service there required subscribers to provide certain information to facilitate salient user-to-user connections. The company may have had other uses for the data it collected, but this possibility did not matter much for the court's purposes. (The question did not make an appearance in the opinions below or on appeal in that case.) At most, the Ninth Circuit in *Roommates* casually observed that the defendant service "ma[d]e *aggressive* use of [user data] in conducting its business," without explaining what "aggressive use" meant.[390] Today, in contrast, service providers structure and elicit user content in far more assertive if innocuous ways. We might wonder whether this, too, might count as making "aggressive use" of content—that is, whether assertive designs

---

*Uses Psychological Tricks to Push Its Drivers' Buttons*, N.Y. TIMES (Apr. 2, 2017), https://www.nytimes.com/interactive/2017/04/02/technology/uber-drivers-psychological-tricks.html (detailing how the company exploits people's tendencies, such as the one to set earnings goals by alerting them that they are "ever so close" to hitting a precious target when they try to log off). This is in sharp contrast to the transparent way in which some online marketplaces own up to their obligations to their agents and employees. *See* Editorial Board, *The Gig Economy's False Promise*, N.Y. TIMES (Apr. 10, 2017), https://www.nytimes.com/2017/04/10/opinion/the-gig-economys-false-promise.html?nytcore-iphone&smid=nytcore-iphone-share ("Uber and other companies use tactics developed by the video game industry to keep drivers on the road when they would prefer to call it a day, raising company revenue while lowering drivers' per-hour earnings.").

[389] *See* John Herrman, *Platform Companies Are Becoming More Powerful – but What Exactly Do They Want?*, N.Y. TIMES (Mar. 21, 2017), https://www.nytimes.com/2017/03/21/magazine/platform-companies-are-becoming-more-powerful-but-what-exactly-do-they-want.html?_r=0 ("With a rigidly structured platform like Uber, for which the company sets prices, the economic problems are somewhat akin to those of a command economy: How low can we push the cost of a ride before drivers stop participating?").

[390] Fair Hous. Council of San Fernando Valley v. Roommates.Com, 521 F.3d 1157, 1172 (9th Cir. 2008) (emphasis added).

might count as "material contribution" under the doctrine.[391]

The immunity may also be inapplicable if the defendant intermediary designs its service in order to profit from user content through some other service. Thus, while Section 230 might require a court to dismiss a suit in which plaintiff alleges that a service provider's "Terms of Use" give the provider an ownership interest in a third party's content,[392] the immunity could very well be unavailable if the service designs its application in order to collect particular kinds of illicit information that, through algorithmic analysis and sorting, it then repurposes in an ancillary or secondary market. In these arrangements, it is a stretch to refer to this manipulation and exploitation of user content as "publishing" within the meaning of the statute.

The rule in *Batzel* that providers attend to whether the third-party user at issue intended to have his or her content published is helpful in puzzling through the question. A court in the Northern District of California, for example, rejected Facebook's Section 230 defense in a case in which users alleged that the social media company misappropriated their names, likenesses, and "likes" for targeted commercial endorsements without their consent.[393] Facebook, the district court in that case explained, grouped plaintiffs' information with advertisers logos, "transform[ing] the character of Plaintiffs' words, photographs, and actions into a commercial endorsement to which they did not consent."[394]

This returns us to the example of Facebook's advertising service. Recall that, there, Facebook enables users to craft microtargeted advertising campaigns to exclude or include prospective audiences on a variety of dimensions, including by "ethnic" or "multicultural affinities." These categories would be uncontroversial but for federal and state laws that prohibit the use of race or ethnicity (and proxies for those attributes) to discriminate against buyers or sellers in the housing and employment market. The same laws bar advertisements that discriminate on those bases.

The pertinent question is whether Facebook is immune from liability under Section 230 for discriminatory advertising campaigns that target or exclude people with ethnic or multicultural affinities. There would be little

---

[391] I do not take up here the point that the source code "controls" the development of user content. *See* Opperman v. Path, Inc., 84 F. Supp. 3d 962, 972 (N.D. Cal. 2015) (detailing how Apple controls which apps are available on the App Store).

[392] *See, e.g.*, Small Justice v. XCentric Ventures, 99 F. Supp. 3d 190, 197 (D. Mass. 2015) (concluding that the transfer of copyright ownership is valid when the user is on inquiry notice of the terms and conditions); Facebook v. Finkel, No. 102578, 2009 WL 3240365, at *1 (N.Y. Sup. Sept. 15, 2009) (holding that the argument that Facebook's Terms of Use grant the user an ownership interest in the content is meritless).

[393] Fraley v. Facebook, 830 F. Supp. 2d 785, 802 (N.D. Cal. 2011).

[394] *Id.* at 802–03.

controversy on the question if, through the advertising service, Facebook required all house- and apartment-hunters to share racial, ethnic, or gender information about themselves or just enabled advertisers to exclude users based on that information. In that scenario, after *Roommates*, Facebook would almost certainly be subject to liability under the FHA. The social media company would likely be even more exposed to liability if it required its social media users to share race or ethnicity (or any information indicating membership in a protected class) even if those users never used the advertising service.

Facebook, however, is not so brazen. It does not *require* participants on the advertising platform or through the social media application to share prohibited information. Nor does it publish all the information it receives; it publishes only a fraction of the user information that it collects, analyzes, and classifies. Relying on algorithms for understanding "big data," Facebook sorts users on a variety of salient dimensions—by, for example, hobby, communities of interest, and profession. This is the same process that enables its flagship social media site to recommend new friends, curate news and current events, and post targeted advertisements for each user. Affinity designations are just one way of articulating the data that it collects and analyzes.

Practically, it was inevitable that Facebook would enable advertisers to microtarget audiences. After all, this is what effective advertisers and marketing directors do anyway in practically all markets. Facebook's great advantage is that it sits atop an extraordinary trove of user data through which it can make marketing across substantive areas more efficient and effective than ever. A publisher of Urdu language books would not want to reach anyone other than Pakistanis or, better, people with an affinity for Pakistani culture. A costume designer would be right to target women with an affinity for soca music during carnival season. A nonprofit that is hosting a career fair for Latinos in New York City should probably target New Yorkers with an affinity for the Dominican Republic. A merchant who sells hair care products for black women will reasonably target those women at the exclusion of others.[395] The advertising service is just one way of sorting pertinent user data to aid small businesses, product managers, and individual users in practical ways.

But does Section 230 shield Facebook from liability for enabling users or advertisers to discriminate against protected classes in markets that are only tenuously tied to the social media service? Or, what is more, may Facebook claim the immunity when it analyzes and clusters the data in ways that users could not foresee or, perhaps, desire? There are several

---

[395] *See* Christian Martinez, *Driving Relevance and Inclusion with Multicultural Marketing*, FACEBOOK NEWSROOM (Oct. 28, 2016), https://newsroom.fb.com/news/h/driving-relevance-and-inclusion-with-multicultural-marketing/.

reasons to believe that the company would be protected under the statute. First, it is not at all obvious that the ethnic or multicultural affinity classification is an actionable proxy for race or ethnicity, as it theoretically could include users of all racial and ethnic backgrounds. Sorting users by affinity rather than race or ethnicity is not the same as sorting on ethnicity or race as such. In any event, unlike the service at issue in *Roommates*, Facebook's advertising service does not require that users share prohibited information about themselves. Nor does it require users to express preferences for races or ethnicities. Its algorithms do the work of sorting. Facebook leaves it to advertisers to decide the uses to which they put the service and affinity classifications. This use-agnosticism suggests that the service is a neutral tool for user-to-user interaction and commerce in the way envisioned under the prevailing doctrine.

On the other hand, a fair housing or equal employment challenge to Facebook's advertising service could cite *Roommates* (and *Carafano*) to argue that the ethnic or multicultural affinity designations make the violation of civil rights laws possible. The company materially contributes to discriminatory online conduct because the Facebook-created affinity classifications are essential to actualizing illegal online conduct.[396] The company's design implicates it in all discriminatory advertising campaigns. Under this theory, Facebook would be subject to what I have called above *design* liability, in contrast to publisher or distributor liability.[397]

That the company collects and synthesizes non-racial or non-ethnic user data to create "ethnic" or "multicultural affinity" classifications does not necessarily justify the immunity. To the contrary, Facebook's use of big data algorithmic analysis of ostensibly non-racial data is precisely the

---

[396] *See* Fair Hous. Council of San Fernando Valley v. Roommates.Com, 521 F.3d 1157 (9th Cir. 2008); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003).

[397] *See supra* Section IV.A. Framed in this way, we might think that prevailing norms in the law of product liability might have something to teach. I do not offer here any meaningful comparison. One worthwhile consideration here is how or even whether the manufacturer of a defective product is legally implicated in an injury to a plaintiff by a third party's illegal use of the defective product. Public law immunity for gun manufacturers comes to mind. *See* Soto v. Bushmaster Firearms International, FBTCV 156048103S, 2016 WL 8115354, at * 23 (Conn. Super. Ct. Oct. 14, 2016) (applying immunity under Protection of Lawful Commerce in Arms Act, 15 U.S.C. § 7901-7903). This is in contrast to the affirmative duty of web developers to accommodate all users of their online service under the Americans with Disabilities Act. *See* Nat'l Fed. of the Blind v. Target Corp., 452 F. Supp. 2d 946, 956 (N.D. Cal. 2006) (rejecting defendant's argument that access to public accommodation is limited to physical access). Some courts have found online services to be outside of the scope of the ADA. *E.g.*, Earll v. eBay, Inc., 599 Fed. Appx. 695, 696 (9th Cir. 2015); Young v. Facebook, Inc., 790 F. Supp. 2d 1110, 1118–19 (N.D. Cal 2011); Oullette v. Viacom, No. CV 10–133–M–DWM–JCL, 2011 WL 1882780, at *7 (M.D. Mont. Mar. 31, 2011). Others have not. *E.g.*, Nat'l Fed. of the Blind v. Scribd., 162 F. Supp. 3d 565, 576 (D. Vt. 2015); Nat'l Ass'n of the Deaf v. Netflix, Inc., 869 F. Supp. 2d 196, 208 (D. Mass. 2012).

sort of thing on which we would expect bigots to rely to mask their true intentions. Facebook also collects user data through its flagship social media application that it, in turn, exploits in the ancillary advertising service. The company's contribution to the unlawful online discriminatory conduct is material—indeed, indispensable—because, through the power of its algorithmic processing, it creates commercially salient classifications that were indiscernible before the intervention. What is more, the purposes to which user content are put are arguably unrelated to the services to which users volunteer their information in the first instance. To put this in the terms of the doctrine, it might be unreasonable for Facebook to expect users to provide personal information about themselves (including data that is not intuitively racial or ethnic) that could later be used to discriminate against them or others on the basis of race or proxies for race.[398]

### B. *Public Duties*

There is at least one other consideration that counsels against immunizing Facebook for discriminatory advertising campaigns that violate the FHA. As *Roommates* and *Accusearch* illustrate, plaintiffs who are not directly injured by a discrete volitional act by a third-party user may still overcome Section 230 to the extent that the defendant service creates or develops prohibited content by design. This feature in the doctrine enables parties to stand in as a representative of the public. Thus, Roommates could not claim the immunity because it elicited and published FHA-prohibited content. Accusearch was not immune because it contracted with researchers to violate consumer privacy laws. In both cases, the injury was not to a discrete party as much as to the public in general. These were cases in which defendant services engaged in what Jack Balkin has called "algorithmic nuisance[s]," the "socially unjustified use of computational capacities that externalizes costs onto innocent others."[399] Thus, in both cases, plaintiffs—a civil rights organization and a federal agency—stood in on behalf of the public.

Generally, as I show at the end of Section II.D above, the immunity does not shield services from liability for violating a duty that they owe to their individual users.[400] But services also are not entitled to protection

---

[398] *Compare* Batzel v. Smith, 333 F.3d 1018, 1032 (9th Cir. 2003) (involving a user who provided his email without intending for the email to be publicly available), *with* Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 802 (N.D. Cal. 2011) (addressing a plaintiff who claimed Facebook "creates content by deceptively mistranslating members' actions").

[399] Jack M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. (forthcoming 2017).

[400] *See supra* Part II (discussing *Barnes v. Yahoo*); *see also* Goddard v. Google, 640 F. Supp. 2d 1193, 1200 (N.D. Cal. 2009) (immunity does not apply to "conduct giving rise to an independent and enforceable contractual obligation"); Universal Communications Systems v. Lycos, Inc., 478 F.3d 413, 419 (1st Cir. 2007) ("[A]n interactive computer service provider remains liable for its own speech.").

from liability under Section 230 when they engage in conduct that is against manifest public law. Thus, the courts in *Roommates* and *Accusearch* rejected the immunity for the defendant services in those cases because the defendants violated public law on housing discrimination and unfair trade practices.[401]

In some regards, the opinions in those cases just restated Section 230's plain terms that services are not immune from liability for creating or developing illegal content "in whole or in part."[402] But the nature of the legal duties that gave rise to potential liability in those cases moved them out of the *Zeran* framework (i.e., injury to plaintiff arising from a discrete volitional act by a third-party user) because plaintiffs' claims in those cases arose from the obligations the defendants owed by virtue of public law. The complaining parties in these cases were a civil rights organization and a government agency.[403] Plaintiffs could have been any party that could stand in for the public.[404] Thus, based on this idea, as unstated as it is, courts have rejected the Section 230 defense in a variety of very recent cases when the defendant provider engages in conduct that directly violates strict federal prohibitions.[405]

## CONCLUSION

Immunity doctrine under Section 230 rests on an outdated view of how most online intermediaries do business. Today, most providers do not solely relay messages or make connections, uninterested in what their users say or do. The largest and most popular applications today collect,

---

[401] *See, e.g.*, FTC v. Accusearch, Inc., 570 F.3d 1187, 1193 (10th Cir. 2009) (describing the FTC suit against online service for engaging in "unfair trade practices under" the Federal Trade Commission Act); Fair Hous. Council of San Fernando Valley v. Roommates.Com, 521 F.3d 1157, 1175 (9th Cir. 2008) (describing a suit against an online operator for distributing third-party information in violation of federal and state housing laws).

[402] 47 U.S.C. § 230(f)(3).

[403] *See, e.g.*, *Accusearch*, 570 F.3d at 1193 (describing the FTC suit against online service for engaging in "unfair trade practices under" the Federal Trade Commission Act); Goddard, 640 F. Supp. 2d at 1195 (outlining an individual suit on behalf of herself and "a class of similarly situated individuals").

[404] Consider civil rights cases in which courts have recognized parties acting as a private attorney general in furtherance of the public interest. *E.g.*, Newman v. Piggie Park Enterprises, 390 U.S. 400, 402 (1968).

[405] *See, e.g.*, Nunes v. Twitter, Inc., No. 14-CV-02843-VC, 2016 WL 3660526, at *1, *8 (N.D. Cal. July 1, 2016) (holding Twitter is not immune from liability in a class action suit brought under the Telephone Consumer Protection Act for unwanted tweets); Sherman v. Yahoo! Inc., 997 F. Supp. 2d 1129, 1137–38 (S.D. Cal. 2014) (finding the "good Samaritan" immunity inapplicable because Yahoo! did not analyze content for offensive or harmful material); Perkins v. Linkedin Corp., 53 F. Supp. 3d 1222, 1225, 1245–49 (N.D. Cal. 2014) (ruling that LinkedIn is not immune for liability in a class action alleging that the social network had improperly harvested users' emails and then used those emails to send messages to other people); Opperman v. Path, Inc., 87 F. Supp. 3d 1018, 1042–45 (N.D. Cal. 2014) (refusing to dismiss similar claims against Apple).

exhaustively analyze, repackage, and then republish customer information. And they engineer users' online experiences to elicit as much information as possible. There is nothing passive or indifferent in any of this. There is certainly nothing in this that resembles "publishing."

This is not an indictment of the activity or business model that the largest and most popular intermediaries provide. But it does suggest that courts ought to rethink the scope of the immunity under Section 230 in a way that is adapted to the oversized influence that online applications and marketplaces have on users' online conduct today. It may be that it does not matter what we call them— publishers or designers of user content—if they are soliciting and curating and editing illicit material. But courts, this Article proposes, should be far more attentive to the designs that determine online content than the prevailing doctrine has allowed to this point. They should shield providers from liability for third-party online conduct only to the extent such providers truly operate as conduits or, as the statute provides, they voluntarily act in good faith as Good Samaritans in the interest of protecting the vulnerable among us.