Policy Analysis

CATO INSTITUTE

January 26, 2021 | Number 906

Circumventing Section 230

Product Liability Lawsuits Threaten Internet Speech

By Will Duffield

EXECUTIVE SUMMARY

Over the past decade, social media platforms have radically expanded our ability to communicate and transact with one another. Privately owned apps and websites provide spaces for every conceivable sort of human interaction on a hitherto unimaginable scale.

As a matter of law, these platforms cannot be treated as the speaker of their users' speech; Section 230 of the Communications Act places liability for hosted content on its creator. This statute ensures that Americans are served by a wide range of digital publishing platforms. Far from a handout, it should be considered a restatement of the First Amendment's free speech guarantee for the Internet Age.

Although Section 230 enables the creation of tools integral to the exercise of free speech, this intermediary liability protection is increasingly seen as a special protection for industry. Several innovative lawsuits threaten to circumvent Section 230's protections by alleging that platforms' scale and ease of use constitute negligent design. These lawsuits present a novel threat to Americans' access to digital publishing tools by offering a sweeping theory of liability that contravenes the purpose of existing intermediary liability protections. If accepted, the claims would open the door to the continual redesign of social media platforms by lawsuit, limiting and frustrating Americans' use of the internet.

Will Duffield is a policy analyst in the Cato Institute's Center for Representative Government, where he studies speech and internet governance.

> "Section 230 was intended to enhance Americans' speech rights by ensuring the availability of 'interactive computer services' such as forums and message boards, precursors to contemporary social media platforms."

INTRODUCTION

Social media platforms are easily accessible digital tools that help users communicate with one another. While their creators may exercise some control over their uses, control is costly, and the responsibility for specific platform uses ultimately rests with individual users. The expectation of user responsibility, which Congress codified in U.S. law in 1996 as Section 230 of the Communications Act of 1934, maximizes the ability of platforms to host speech.

Although Section 230 is often understood as a protection for industry, its chief beneficiaries are internet users. Americans' ability to exercise their First Amendment rights on the internet depends on the availability of publishing tools that social media platforms provide. Section 230 was intended to enhance Americans' speech rights by ensuring the availability of "interactive computer services" such as forums and message boards, precursors to contemporary social media platforms.

This policy analysis applies an understanding of Section 230 as a protection for social media platforms as neutral tools—intended to ensure their wide availability—to the theories of liability proffered in two recent lawsuits, *Herrick v. Grindr LLC* and *Daniel v. Armslist LLC*. These suits attempt to hold platforms liable for the malicious actions of their users. The sweeping standard of negligence proposed in these cases ignores the relationship between the availability of internet platforms and the ability to exercise First Amendment rights that undergirds Section 230. This paper examines how courts have recognized this relationship in dismissing these novel claims and analyzes legislative proposals to require "reasonable moderation" of social media, an idea that these suits have inspired. If the provision of easily accessible publishing tools is considered negligent, Americans' practical ability to speak using the internet would be severely hampered.

NEUTRAL TOOLS

From social media platforms such as Facebook, Twitter, and YouTube to the digital marketplaces hosted by Amazon and eBay, our modern internet is a network of intermediaries. These intermediaries provide value to consumers by developing and managing sets of neutral tools that are part creative studio, part matching service. They allow users to both create content—establishing personal profiles or editing photos—and discover content via search tools and algorithmically selected newsfeeds. The character of these tools may vary; Snapchat, for example, offers image editing software with inbuilt sharing and deletion functions, while Uber uses an algorithm to match riders and drivers.

Platforms need users to give life to their tools. Uber does not own cars or employ drivers, and Snapchat does not create the images that users share in its app. Rather, the platforms rely on others to make use of their tools and, in so doing, render their networks attractive to additional users.

Within the context of social media, neutral tools are platform-provided features that can be used for both lawful and unlawful purposes. Crucially, they are open and accessible; utilizing them rarely requires more than the creation of an account. Neutral tools must have some lawful purpose or use, even if they can be misused to illegal ends. While their openness renders them equally available to both good and bad actors, in most instances such tools are used for legitimate, and often innocuous, purposes.

Unfortunately, misuses of these tools tend to receive far more attention than their unremarkable employment in the commerce of everyday life, and their open nature makes it difficult to exclude bad actors. Think again of Uber: Anyone can sign up for an account and use the service to be matched with a driver who will ferry them to a destination, such as a place of employment, home, or a friend's party. But bank robbers have attempted to use Uber to summon getaway vehicles.[1]

A service or tool that does not have lawful purposes, such as SilkRoad, a now-defunct online market for illicit drugs, would not be considered a neutral tool in this sense.[2] Though it might have been possible to use

Silk Road lawfully, the platform was so overwhelmingly oriented toward illegal commerce that it was denied Section 230's protections. Addressing SilkRoad's Section 230 defense in 2014, Southern District of New York Judge Katherine Forrest wrote that "even a quick reading of the statute makes it clear that it is not intended to apply to the type of intentional and criminal acts alleged to have occurred here."[3]

Digital neutral tools have much in common with what we might think of as analog neutral tools, such as a hammer or Geiger counter. They have some intended lawful use, but individual end users determine how to employ them, discovering unintended uses both legitimate and illegitimate. For example, a hammer could be used, as intended, to drive nails. It could also be employed in a useful but unintended capacity as a paperweight. But it could also be used to hit someone—a violent, unintended, and almost always unlawful application. As a matter of law, we do not hold the makers of hammers responsible for the actions of people who use hammers as weapons, nor do we fault the hammer-makers for failing to build hammers incapable of being used as weapons. Likewise, were a Geiger counter used in the theft of radioactive material, we would not blame its manufacturer. However, unlike toolmakers and sellers such as the blacksmith and Sears and Roebuck of old, the creators of digital neutral tools have some ostensible ability to prevent bad actors from continuing to use their tools.

Novel Opportunities for Revocation?

Historically, some uses of analog tools were contractually prohibited, but restrictions were rare and difficult to enforce. For example, a photocopier might come with a license agreement indicating that it is not to be modified or used to replicate copyrighted works; however, the manufacturer cannot effectively prevent purchasers from photocopying *Harry Potter*. In contrast, digital neutral tools are regularly subject to rules that dictate how they can be used. Furthermore, unlike contractual restrictions, which must be enforced by a court, a social media platform may revoke a user's access unilaterally.

The creators of digital tools manage their products in an ongoing fashion: adding new features, ensuring continued compatibility with other tools, and policing misuse. These efforts are principally intended to keep social media platforms running smoothly, allowing users to enjoy the underlying service without being driven off by trolling and harassment. Though content moderation may limit the harms experienced by third parties as a result of platform misuse, it is far from infallible. Nevertheless, the capacity to moderate might be seen to create an associated responsibility on the part of platforms. After all, if platforms can prevent misuse, perhaps they should be required to do so.

But consider the challenges that content moderators face: The scale of contemporary social media platforms is unlike anything in human history. Apple's App Store hosts two million apps.[4] Facebook's 2.4 billion users exchange roughly 100 billion messages a day.[5] YouTube users upload over 400 hours of video to the platform every minute.[6] This scale makes uniform governance extremely difficult. Platforms cannot prescreen uses of their tools; the review queues would stretch forever. Nor can they review everything their users publish; even post-publication, there is simply too much content. While firms maintain extensive rules governing the use of their products (usually called community standards) and can terminate specific user accounts at will, enforcing these rules is an endless and unforgiving task. Therefore, most platforms rely on some combination of user and algorithmic flagging, paired with review by human moderators.

Although this approach allows platforms to identify and address some of the most egregious misuses of their tools, it is far from foolproof. Unless wholly moderated by algorithm, content can be addressed only after it has been posted. Reliance on user flagging introduces opportunities for bad actors to game the moderation system, and well-trained human reviewers still make mistakes and misinterpret

"Though content moderation may limit the harms experienced by third parties as a result of platform misuse, it is far from infallible."

“Given platforms’ limited ability to police misuses of their tools and the high costs inherent in trying for perfect enforcement, opportunities to moderate content should not impose responsibilities to do so.”

guidelines.[7] Even with a false-positive rate of less than 1 percent, a platform that reviews billions of messages every day would incorrectly flag millions of messages as undesirable. Increasing the sensitivity of flagging algorithms would scoop up more benign content. Hiring an ever-increasing number of human moderators is expensive, drawing resources from the development of the underlying service, and might exacerbate the effects of human biases on moderation outcomes. Most firms have responded to demands for increased moderation by relying more heavily on algorithmic filtering. Though this is the easiest way to address the unique demands of moderation at scale, algorithmic moderation is often opaque and has difficulty appreciating the local norms and contexts of diverse internet communities.

Misuse could be addressed by more strictly prescreening *users* rather than specific uses. However, increasing the barriers to platform entry would prevent many people from using the platform, thereby reducing the value of its network. When Facebook first launched, it restricted membership to people with Harvard email addresses. Collegiate Facebook was undoubtedly easier to govern than global Facebook. However, collegiate Facebook was less useful, even for college students, because they were unable to use it to talk to their noncollegiate friends and family. Limiting scale may limit harm, but it limits utility as well. Furthermore, identity verification requirements exclude those without government-issued identification and may threaten user anonymity and privacy.[8]

Although the creators of contemporary digital tools have some ability to police the use of their products, this capability is far from perfect. Importantly, improvements in community standards enforcement are not without tradeoffs. At the margin, improved enforcement increases platform costs and false positives. At some point far short of perfect moderation, these costs to the varied legitimate uses of digital tools would outweigh the benefits of improved enforcement. If several human moderators from varied cultural backgrounds prescreened every Facebook post, it is unlikely that Facebook would host much harmful content. But then, Facebook probably would not have much content at all. The extreme of perfect safety would be accompanied by perfect uselessness.

PROTECTIONS FOR NEUTRAL TOOLS

Given platforms’ limited ability to police misuses of their tools and the high costs inherent in trying for perfect enforcement, opportunities to moderate content should not impose responsibilities to do so. Under current U.S. law, they do not. With a few exceptions, digital intermediaries cannot be held liable for content posted by their users. If I use Facebook to publish a libelous claim about Rep. Devin Nunes (R-CA), I can be sued for libeling Nunes, but he cannot hold Facebook liable for retransmitting my sentiments or failing to prevent me from using the platform to libel him. Section 230(c)(1) prevents the “provider or user of an interactive computer service” from being “treated as the publisher or speaker of any information provided by another information content provider.”[9] It most commonly protects social media platforms from claims arising from some third party’s use of the platform’s publishing suite. Allowing Nunes to sue Facebook would treat the social media platform as the “publisher or speaker” of my speech.

Though Section 230(c)(1)’s intermediary liability protections are most often implicated in republication claims, the statute’s language applies more broadly. So long as the services and tools offered by the “providers of an interactive computer service” have legitimate purposes, and so long as the providers do not take part in the creation of the content in question, Section 230 prevents the managers of these tools from being held liable for others’ misuse of their products.[10]

Section 230 is often understood merely as a protection against liability for third-party

speech. However, because most claims arising from the misuse of a publishing platform can be reduced to speech claims, Section 230(c)(1) is more broadly applicable. Because the statute prevents platforms or tool providers from being treated as the speaker or publisher of "any information" provided by another, it forecloses misuse-based claims provided that the alleged harms stem from some platform use of user-generated content. This might include information processed by a tool but never widely "published" by the service, such as the current location of your Uber driver.

The law further indemnifies intermediaries against claims arising from their private moderation efforts, ensuring that litigious users will not circumscribe platforms' attempts to police their services. Under Section 230 (c)(2), "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." The statute's "otherwise objectionable" language gives platforms wide latitude in setting rules to foster digital communities with particular purposes. Although some policies may be unpopular or impractical, as a matter of law, social media firms are given free rein to govern their platforms as they wish.

Before Section 230

Section 230's twin protections were spurred by a pair of judicial decisions that, when taken together, created perverse incentives for early platforms' moderation efforts. In 1991, Cubby Inc., the publisher of an early electronic newsletter called *Scuttlebutt*, responded to defamatory claims that a competitor, *Rumorville*, made about Cubby's CEO, suing both *Rumorville* and its digital host, CompuServe Inc., in the Southern District Court of New York.[11] Traditionally, CompuServe might have been seen as either a publisher, subject to strict liability for its product, or a distributor, liable only to the extent that it "knew or had reason to know" that its offerings were defamatory.[12] However, the court held that because CompuServe neither exercised editorial control nor conducted any sort of review of *Rumorville*'s postings, CompuServe was not liable for *Rumorville*'s content. "CompuServe has no opportunity to review *Rumorville*'s contents before [*Rumorville*'s parent company] 'uploads' it into CompuServe's computer banks, from which it is instantaneously available to approved [CompuServe Internet Service] subscribers."[13] *Cubby Inc. v. CompuServe Inc.* extended distributor liability to digital intermediaries that exercised little or no editorial control over third-party content, offering them the protections traditionally granted to newsstands and booksellers. This protected CompuServe from Cubby's defamation claim, though it left open the possibility that CompuServe might have been liable for *Rumorville*'s defamation had it failed to act after being made aware of the defamatory content.

In 1995, Stratton Oakmont Inc., the brokerage firm of *Wolf of Wall Street* fame, sued internet service Prodigy Services Co. in New York state court after a user of the service's Money Talk message board posted several screeds alleging that Stratton Oakmont's directors were about to be indicted. Unlike CompuServe, Prodigy was attempting to run a family-friendly business. Prodigy had promised users that it would remove "obscene, profane, or otherwise offensive" messages and promulgated "content guidelines" prohibiting pseudonymous accounts and defamation.[14] Prodigy sought to walk back its marketing claims in court, contending that "in terms of sheer volume—currently 60,000 messages a day are posted on Prodigy bulletin boards—manual review of messages is not feasible." In a break from the *Cubby Inc.* holding, New York Supreme Court Justice Stuart Ain ruled that by "actively utilizing technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness," Prodigy was "clearly making decisions as to content and such decisions constitute editorial control,"

"Because most claims arising from the misuse of a publishing platform can be reduced to speech claims, Section 230(c)(1) is more broadly applicable."

> "In accommodating *Auvil*, Ain imposed liability on Prodigy because of its decision to moderate rather than its capacity to do so."

rendering it a publisher, liable for whatever appeared on its message boards.[15]

In *Cubby v. CompuServe*, a platform that made no effort to moderate user-generated content was protected as a mere distributor, while in *Stratton Oakmont Inc. v. Prodigy Services Co.*, the court found that a bulletin board could be held liable for third-party speech because of its content moderation efforts. Taken together, these decisions created a "moderator's dilemma," perversely rewarding platforms that made no attempt to limit the misuse of their tools while punishing those that attempted moderation when their efforts were not met with perfect success. If any attempt to moderate content rendered platform managers responsible for all third-party misuses of their tools, few platforms would engage in content moderation.

While most discussion of the *Cubby* and *Stratton Oakmont* cases concerns their creation of the "moderator's dilemma," it is worth examining an aspect of *Stratton Oakmont* that has received less attention. Justice Ain cited the 1992 case *Auvil v. CBS "60 Minutes"* to justify his imposition of liability on Prodigy. *Auvil* concerned the responsibility of affiliate television stations to police content provided by their networks. Ain reasoned that Prodigy should be treated differently than the affiliate stations in *Auvil* because Prodigy had affirmatively chosen to moderate. "In contrast, here Prodigy has virtually created an editorial staff" that "monitor incoming transmissions and in fact do spend time censoring notes."[16] Thus, although the ruling created perverse incentives, in accommodating *Auvil* Ain imposed liability on Prodigy because of its decision to moderate rather than its capacity to do so. According to Ain, "It is Prodigy's own policies, technology and staffing decisions which have altered the scenario and mandated the finding that it is a publisher."

Auvil held that although affiliates could technically and contractually refrain from retransmitting network content, requiring them to take responsibility for said content would impose unrealistic burdens. According to that decision:

> Plaintiffs' construction would force the creation of full-time editorial boards at local stations throughout the country which possess sufficient knowledge, legal acumen and access to experts to continually monitor incoming transmissions and exercise on-the-spot discretionary calls or face $75 million dollar [sic] lawsuits at every turn. That is not realistic.[17]

The *Auvil* decision further specified that the imposition of intermediary liability would circumscribe both "media's right of expression and the public's right to know."[18] The court recognized that imposing liability on speech intermediaries could have repercussions for the rights of both speakers and listeners.

Auvil is one illustration that, in the words of policy analysts Brent Skorup and Jennifer Huddleston, "even before the creation of Section 230, many courts had shifted from the strict liability regime toward conduit liability protections and fault-based requirements."[19] Even after *Stratton Oakmont*, an intermediary's technical capacity to moderate third-party content did not necessarily create a responsibility or obligation to do so, especially if moderation would diminish the expressive value of its service.

In 1995, Reps. Ron Wyden (D-OR) and Chris Cox (R-CA) sought to rectify the consequences of *Stratton Oakmont* and *Cubby* by both indemnifying platforms against claims arising from user-submitted content and empowering them to moderate their platforms. Their solution, originally proposed as the Internet Freedom and Family Empowerment Act, was included in the Telecommunications Act of 1996 as an amendment to an anti-pornography statute known as the Communications Decency Act. The Wyden-Cox amendment was adopted as a compromise between internet speech advocates and anti-obscenity activists led by Sen. J. J. Exon (D-NE).[20] When the Supreme Court later invalidated Exon's pornography restriction provisions in *Reno v. American Civil Liberties Union*, the Wyden-Cox amendment to the Communication Decency

Act, now Section 230, was all that was left.[21] The congressional findings that accompany the bill illustrate the drafters' belief that, as the internet grew and Americans' everyday activities moved online, their ability to speak, socialize, and transact would depend on the availability of internet platforms. One finding reads, "Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services." Crucially, Wyden and Cox recognized that, when taken as a whole, "the Internet and other interactive computer services" could provide "a forum for a true diversity of political discourse."[22] They did not expect every website to host every sort of speech but understood that so long as new platforms could spring up to meet users' needs and were not hobbled by costly litigation, the internet could provide a home for even disfavored speech.

Handouts for Whom?

In the two decades following the passage of Section 230, the internet's tremendous growth has transformed the statute from a little-known protection for an infant industry to the legal basis for a seemingly all-encompassing internet of intermediaries that suffuses our daily lives. Section 230 allows the tools and services we rely upon—from messaging apps to mobile payment services—to operate despite their imperfect moderation efforts. As previously illustrated, attempts at perfect moderation are costly. A platform moderation regime that sought to prevent all misuses of its tools would have to accept incredibly high false-positive rates and significant barriers to platform access.

While platform users benefit tremendously from Section 230, it is often denounced as a protection for industry or, in the parlance of many critics, "Big Tech." Because Section 230 is a specific statutory protection for the providers of interactive computer services, it is increasingly described as a "handout" to technology firms, an undeserved benefit free of reciprocal obligations or broader public benefit. Partisans of many stripes have taken up the language, albeit for contrary reasons. Republicans worry that these tools are not, in fact, open to all but are instead governed with bias against conservatives. Democrats fear that platforms' imperfect moderation and algorithmic discovery functions provide potent channels for the spread of hateful sentiment and misinformation. Speaker Nancy Pelosi (D-CA) has taken to calling Section 230 a "gift" to tech companies.[23] On the right, Sen. Josh Hawley (R-MO) deems it "a sweetheart deal that no other industry enjoys."[24] *Breitbart*'s Allum Bokhari describes it as "the golden government handout that has allowed online companies like Google to prosper."[25]

Bokhari is partially correct; it is unlikely that Google could exist in its current form without Section 230. However, Google is far from the only, or even the primary, beneficiary of Section 230.

When we use social media platforms to interact, whether talking to friends on WhatsApp, arguing about politics with strangers on Twitter, or responding to a used boat advertisement on Craigslist, we are engaging in activity protected by the First Amendment. Platforms are not bound by the First Amendment and remain free to police our use of their services as they see fit. The government, however, cannot censor speech on the internet any more than it can censor speech elsewhere.[26] While our rights do not grow or shrink in response to technological advances, social media has greatly enhanced our ability to exercise our First Amendment rights. Private firms have developed countless digital tools serving a myriad of interests. Every tool cannot be expected to serve everyone: in many cases, design or governance decisions intended to better provide for some activities may foreclose others. Nevertheless, the platform ecosystem, taken as a whole, provides at least a minimally viable home for almost all interests. However, we are able to exercise our speech rights within this ecosystem only because Section 230 provides a legal framework for its existence.

If the manufacturers of movable type had been held liable for how others arranged

"Section 230 allows the tools and services we rely upon—from messaging apps to mobile payment services—to operate despite their imperfect moderation efforts."

> "If Section 230 is understood as a 'handout,' it must be appreciated as a handout to speakers and listeners: a gift to anyone using internet platforms or benefiting from anyone else's use of them."

their letters, few printing presses would have been manufactured. In the Ottoman Empire, a combination of the dominance of scribal culture and regulatory uncertainty inhibited the provision of printing services and, in turn, discourse in the printed word for hundreds of years.[27] If Section 230 is understood as a "handout," it must be appreciated as a handout to speakers and listeners: a gift to anyone using internet platforms or benefiting from anyone else's use of them. The greatest beneficiaries of the internet are its users, those billions of souls who grant platforms their unmanageable scale. Limiting speech by limiting the creation of speech tools clearly violates liberal free speech norms.

Likewise, our First Amendment tradition recognizes "the press" as a set of technologies to which the government cannot restrict access.[28] University of California, Los Angeles, law professor Eugene Volokh identifies a host of cases from the 19th century in which the First Amendment was implicated in disputes over individual citizens' publication of comments or complaints via newspaper advertisements, including *People v. Simons*, *In re Austin, Taylor v. Delavan*, and *Brandreth v. Lance*.[29] In *Brandreth*, for example, the New York Chancery Court (the highest court in the state in 1839) invalidated an injunction barring a businessman, Lance, from hiring both a writer and a printer to produce a biography critical of a professional rival. Volokh writes, "Nothing in the court's opinion suggested that the liberty of the press was a right that belonged only to printer Hodges; the injunction was dissolved as to all defendants."[30] This broad definition of the press respects the necessity of the division of labor in speech production. More recently, in its 1964 *New York Times Co. v. Sullivan* decision, the Supreme Court held that the First Amendment protects noncommercial paid republication as it does other speech. The court expressed concern that a ruling to the contrary "might shut off an important outlet for the promulgation of information and ideas by persons who do not themselves have access to publishing facilities—who wish to exercise their freedom of speech even though they are not members of the press."[31] Though the First Amendment does not necessarily provide a right to specific communications technologies, in *New York Times v. Sullivan* the Court recognized a link between the vitality of speech rights and broad access to speech tools.

Thus, protecting speech rights by protecting the creators of publishing tools is entirely in keeping with America's First Amendment tradition. Like other statutory speech protections, Section 230 was passed to rectify judicial trends that threatened to curtail Americans' ability to speak freely.[32] Given that contemporary platforms could not function without Section 230, it serves as a guarantee of free speech rights, authorizing the manufacture of means of expression. It is not the only intermediary liability protection intended to shield constitutionally protected activity.

Far from Unique

While Section 230's critics have labeled it a unique protection afforded only to technology firms, industries similarly linked to the exercise of constitutional rights have received comparable protections. Sen. Ted Cruz (R-TX) claims that Section 230 "provides technology companies with immunity enjoyed by no other industry," but he surely supports similar protections for firearms manufacturers.[33] The Protection of Lawful Commerce in Arms Act (PLCAA) insulates gun manufacturers and sellers from some forms of liability that could arise from the misuse of firearms. It prohibits a wide range of civil and administrative proceedings against "a manufacturer or seller of a qualified product or a trade association, for damages, punitive damages, injunctive or declaratory relief, abatement, restitution, fines, or penalties, or other relief, resulting from the criminal or unlawful misuse of a qualified product by the person or a third party."[34] Qualified products include firearms, ammunition, and the component parts thereof.

The PLCAA's passage was prompted by a series of lawsuits that sought to hold

gun manufacturers liable for end-user misuse, contending that the manufacture and sale of modern firearms constituted negligent behavior.[35] Recognizing that holding gun manufacturers strictly liable for the unlawful use of their products would impede the manufacture of arms and, in turn, limit citizens' ability to exercise their Second Amendment rights, Congress precluded such suits. Defending his vote for the bill, Sen. Bernie Sanders (D-VT) likened firearms to other useful tools, casting manufacturer liability as an inappropriate mechanism for controlling end-user behavior.

> If somebody has a gun and it falls into the hands of a murderer, and that murderer kills somebody with the gun, do you hold the gun manufacturer responsible? Not anymore than you would hold a hammer company responsible if somebody beat somebody over the head with a hammer. That is not what a lawsuit should be about.[36]

The bill's nonbinding findings and purposes sections explicate the relationship between manufacturer liability and ordinary citizens' access to arms. The PLCAA is intended to foreclose "the possibility of imposing liability on an entire industry for harm that is solely caused by others" because such liability "threatens the diminution of a basic constitutional right and civil liberty."[37] Despite providing protections only for the manufacturers of arms, the bill purports to "preserve a citizen's access to a supply of firearms and ammunition." While clearly intended to safeguard the rights of individual citizens, the PLCAA, like Section 230, offers protection only to firms. Nevertheless, in both cases the legislations' benefits accrue to individuals because the effective exercise of their rights hinges on the availability of certain products.

Within the more limited context of the Second Amendment, those products are arms and ammunition. The First Amendment rights of freedom of speech and the press encompass a wider set of activities, utilizing a more expansive set of tools. Section 230's definition of covered tool creators—"the providers of an interactive computer service"—may seem overbroad, but almost everything we do on the internet is reducible to speech. All of the platforms that claim Section 230's protections are, in one way or another, hosting user speech. In this light, far from being a unique corporate handout, Section 230 simply buttresses the First Amendment, ensuring that its guarantees retain their vitality in the Internet Age. It is similar to other speech-enhancing statutes, such as anti-SLAPP laws (or laws that oppose strategic lawsuits against public participation), the Consumer Review Fairness Act, and reporter shield statutes.[38] By providing a process for quickly dismissing meritless defamation suits, prohibiting gag clauses in product terms of use, and preventing the disclosure of journalists' notes and sources, these statutory protections strengthen the First Amendment's guarantee of free speech.

Section 230 should be understood as a guarantee of platform availability, principally intended not to protect intermediaries for their own benefit but to ensure that the services they offer are widely available. This recognition puts in context the threat posed by the recent spate of product liability suits brought against social media platforms and the legislative reform proposals they have inspired.

REDESIGNING PLATFORMS THROUGH PRODUCT LIABILITY

Section 230 has effectively prevented suits attempting to treat digital intermediaries as the speaker of user-submitted content. In response, litigants have shifted their claims. A new wave of lawsuits against digital intermediaries targets their role in providing platforms for unwanted or harmful speech. Rather than attempting to treat platforms as the speakers of actionable third-party speech, these suits cast the platforms' architects as negligent designers, foisting dangerous products on an unsuspecting public. While these novel pleadings may appear to circumvent Section 230's protections, on

"The benefits of the PLCAA and Section 230 accrue to individuals because the effective exercise of their rights hinges on the availability of certain products."

"Grindr's decision to refrain from employing VPN blocking constitutes a product-defining accessibility and safety feature, perfectly within the remit of Section 230."

closer inspection the alleged negligences collapse into speech claims.

Herrick v. Grindr LLC

The most prominent of these product liability cases is *Herrick v. Grindr LLC*, a 2017 lawsuit concerning the responsibility of dating platforms to prevent harassment. The case was eventually appealed to the Supreme Court, which declined to review the lower court's decision in favor of the defendant.

According to court filings, in 2015, Matthew Herrick met his now ex-boyfriend, J.C., on Grindr, a location-based dating app for gay men. After their relationship ended, J.C. began harassing and stalking Herrick. J.C. created a fake Grindr profile in Herrick's name and, posing as Herrick, invited other men to Herrick's home for violent sex. Over a thousand would-be paramours responded to J.C.'s impostor profile, and many harassed Herrick at his home and place of work. Herrick asked Grindr to remove the account and reported the impersonation to the police, eventually filing 14 reports and receiving a protective order against J.C. The protective order went unenforced, however, and J.C. continued to impersonate Herrick.[39] Herrick filed suit against Grindr for failing to prevent his ex-boyfriend from harassing him; months later, the U.S. Department of Justice charged J.C. with cyberstalking in a case that is still ongoing.

Herrick sued Grindr under New York state law, bringing a host of product liability claims. They included a defect in manufacture claim on the grounds that Grindr failed "to incorporate widely used, proven, and common safety software"; a failure to warn claim "because Grindr knew, but failed to warn, that its Grindr App has been and can be used as a stalking weapon"; and more.[40] Grindr removed the case to federal court, where it was initially dismissed on Section 230 grounds.[41] Herrick appealed the dismissal to the Second Circuit.[42] His appeal contended that Section 230 was no bar to recovery because his claims concerned Grindr's design rather than its publication of third-party speech.

Herrick's attorneys argued that Section 230's plain language "does not extend to Grindr's operation and design," treating decisions about how to process and present user-provided information as distinct from publishing. Subsequent arguments attempted to establish a dichotomy between editorial functions and design choices, casting the use of specific automated moderation techniques as "safety processes" as opposed to parts of the publication process. "Obtaining ICC [Interstate Commerce Commission] numbers, MAC [media access control] addresses, utilizing VPN [virtual private networks] blocking and geofencing are all safety processes involving the function of computer code," yet all of these functions work to determine whose speech appears on the platform.[43] Blocking users connecting to the app via VPNs—a process that disguises users' location and identity by routing their traffic through a proxy server—could help to exclude unwanted users attempting to evade past bans from the service, but it would also entirely exclude those who rely on VPNs to circumvent state internet filtering.[44] Given the extent to which intolerant attitudes about homosexuality and illiberal internet censorship tend to accompany one another, Grindr's decision to refrain from employing VPN blocking constitutes a product-defining accessibility and safety feature, perfectly within the remit of Section 230.

Herrick's suit also presents the processing of user data as an act of creation itself: "To the extent that Grindr's conduct in operating and designing its application relates to the publication of content, it is content created by Grindr's geolocation software and the like."[45] GPS data, gathered via a user's handset and transmitted to Grindr with the user's permission and expectation that Grindr will show the information to potential suitors, clearly meets the definition of user-generated content. Under the presented theory of creation, nearly anything done with user-submitted content could render it content "created" by the platform. If the processes required to present one user's location to another constitute a transformative

act of creation, routine functions such as image resizing or the grouping of contacts into a friends list could be considered similarly creative, stripping platforms of the very capabilities for which they are valued.

In March 2019, the Second Circuit upheld the appellate court's dismissal of Herrick's suit, finding that his negligence claims were really speech claims foreclosed by Section 230. The court first addressed the origin of Herrick's injuries, setting aside his product liability arguments. It found that Herrick's injuries were caused by content submitted by his ex-boyfriend. While Herrick's claims ostensibly concern Grindr's lack of safety features, this absence "is only relevant to Herrick's injury to the extent that such features would make it more difficult for his former boyfriend to post impersonating profiles or make it easier for Grindr to remove them."[46] As such, his defect in manufacture claim collapses into a speech claim: if Grindr's purported defect is that it could be used to malicious effect by Herrick's ex, Herrick is attempting to hold Grindr liable as the publisher of his ex's abuse.

Turning to Herrick's claims concerning Grindr's role in creating the impostor profile, the court cites *Fair Housing Council of San Fernando Valley v. Roommates.com LLC*, a case that helped to delineate the outer limits of Section 230's protections.[47] In that case, the roommate matching service Roommates.com was considered to be the "publisher or speaker" of protected category information and preferences that it *required* prospective users to provide.[48] Because the service mandated the provision of the information that rendered its roommate profiles illegally discriminatory, it could not claim that the information was wholly "provided by another." The *Roommates* court chose participation in the creation of illegal content as the threshold for liability precisely to discourage the sort of claims seen in *Herrick v. Grindr*:

> There will always be close cases where a clever lawyer could argue that something the website operator did encouraged the illegality. Such close cases, we believe, must be resolved in favor of immunity, lest we cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites, fighting off claims that they promoted or encouraged—or at least tacitly assented to—the illegality of third parties.[49]

The "duck-bites" line is a particularly appropriate description of the potential effect of *Herrick v. Grindr* and similar cases. Feature-specific suits would not sound a singular death knell for platforms, but they would dismantle the platforms piecemeal. The imposition or withdrawal of features via litigation would regularly upend the user experience. As the list of features mandated by an ever-evolving duty of care grew, diversity within the platform ecosystem would necessarily shrink.

In *Herrick v. Grindr*, Grindr did not contribute to the unlawfulness of J.C.'s impostor profile. J.C.'s submission of fake information about Herrick rendered the profile unlawful, and Grindr's algorithmic presentation of that profile to nearby users did nothing to further contribute to its unlawfulness.

> To the extent that [Herrick's claims] are premised on Grindr's matching and geolocation features, they are likewise barred, because under § 230 an ICS [interactive computer service] "will not be held responsible unless it assisted in the development of what made the content unlawful" and cannot be held liable for providing "neutral assistance" in the form of tools and functionality available equally to bad actors and the app's intended users.[50]

Grindr neutrally provides its users with the tools that allow them to create profiles and find nearby users. Grindr, therefore, cannot be treated as the "publisher or speaker" of resultant user-designed profiles any more than the creator of any other digital tool can be held liable for its uses. Because Herrick's

"Feature-specific suits would not sound a singular death knell for platforms, but they would dismantle the platforms piecemeal."

> "The theory of liability proposed in *Herrick v. Grindr* expected Grindr to rectify what ultimately was a failure of law enforcement."

product liability claims were understood as artfully pled speech claims, and because Grindr did not contribute to the illegality of J.C.'s impostor profile, the Second Circuit denied Herrick's appeal. He further appealed his case to the Supreme Court, which declined to take it.

Nevertheless, *Herrick v. Grindr* should concern us. The theory of liability proposed in *Herrick* expected Grindr to rectify what ultimately was a failure of law enforcement, even if it meant making significant changes to the service. J.C.'s actions likely constitute criminal harassment, cyberstalking, or any number of other clearly defined crimes. When the court granted Herrick a protective order against his ex, the police should have prevented J.C. from harassing him. When J.C. continued to operate the impostor profile in violation of the protective order, the police should have arrested him. They failed to do so. However, a failure of law enforcement should not be exploited in order to place additional responsibilities on Grindr; if anything, the attempt to hold Grindr responsible for J.C.'s actions diverted critical attention that ought to have been directed at the New York City Police Department.

If taken seriously, the theory of liability proposed in *Herrick v. Grindr* would have sweeping repercussions for our internet of intermediaries. Speaking on a panel at the American Enterprise Institute, Boston University professor of law Danielle Citron criticized Grindr's decision to refrain from implementing the "safety processes" demanded in *Herrick v. Grindr*.

> I'm not sure we should feel so badly for Grindr because Grindr tells Michael Herrick that it has no capacity to identify anyone on their site and cannot prevent people from reappearing, which is nonsense. As a technical matter, its inability to trace IP [Internet Protocol] addresses is a design choice.[51]

Grindr's decision to refrain from developing the ability to track users across accounts is certainly a design choice, but it's a reasonable one in the face of competing conceptions of safety. This is a decision that Grindr, not judges or litigants, is best positioned to make. Under the theory of liability proposed in *Herrick v. Grindr*, this decision was not only wrong but dangerous. However, were Grindr to adopt the desired "safety processes," those processes would create other countervailing dangers.

Imagine if Herrick's suit succeeded and Grindr had been required to implement VPN blocking and methods of identifying its users in order to retain intermediary liability protections. First, Grindr users who live in countries that block the application would no longer be able to circumvent state firewalls. For users living in places where homosexuality is stigmatized or criminalized, the ability to discover and screen would-be paramours before meeting them in person is of vital importance. Were Grindr able to effectively identify its users by linking their accounts to subscriber identity module, or SIM, cards or IP addresses, this capability could be co-opted via legal demands or state-sponsored hacking to expose and identify users in Iran or Saudi Arabia, where homosexuality is punishable by death. This is not a decision that should be made without consideration of the tradeoffs between Herrick's safety, given the availability of alternative remedies for Herrick, and the safety of millions of other Grindr users around the world.

Furthermore, these are precisely the design decisions that Congress, through Section 230, explicitly empowered platforms to make. Critics of Grindr's current design present a choice between safety and Grindr's business model, rather than one between competing user demands for safety through moderation and safety through privacy.

> Grindr's business model, they said, would be disserved by changing the architecture of their site, and given how it has been misused, strikes me as, they've created something that's

> ultra-hazardous, and they walk away and they don't care.[52]

Court-ordered changes to platform architecture would be most disruptive to end users, the greatest beneficiaries of intermediary liability protections. Again, the harms Herrick suffered resulted from his ex's willingness to lie with cruel intent while filling out a personal advertisement. He might have used another app such as Tinder, a dating subreddit, or any other publishing platform on which someone might plausibly solicit sex. If Grindr, in establishing a dating platform that could be used anonymously, created something "ultra-hazardous," it is hard to see how other contemporary platforms would not be deemed similarly dangerous. The mere capacity for misuse should not be grounds for the judicial reorganization of an otherwise lawfully useful service, particularly when it is far from clear that the desired changes would not create greater harms.

Herrick's attempt to use product liability claims to get around long-standing Section 230 precedent failed in this case. The court held that Grindr was not liable for failing to prevent J.C.'s illegal use of the platform. A second suit, decided more recently, takes this theory of liability even further, attempting to foreclose platforms' accommodation of legal, constitutionally protected activity on the grounds that it encourages or could provide for dangerous or illegal behavior.

Daniel v. Armslist LLC

Armslist.com is a digital classified advertisement website for firearms.[53] It allows users to post ads for firearms that they wish to sell and provides a search tool to help would-be buyers sort through listings. In October 2012, Radcliffe Haughton entered a spa in Brookfield, Wisconsin, and shot seven people, including his ex-wife, Zina Daniel Haughton, before turning his gun on himself.[54] He could not lawfully purchase a firearm because of a restraining order, but he had posted a "want to buy" ad on Armslist and used the service to find a private seller from whom he purchased a handgun.

As opposed to those formally in the business of selling guns, individuals wishing to sell a personally owned firearm in most states are not required to perform background checks on prospective buyers. In 2016, Yasmeen Daniel, Zina's daughter, brought suit against Armslist, alleging that the "design and operational features" of Armslist negligently encouraged illegal sales to persons prohibited from owning firearms.[55] Unlike many other intermediary liability cases, this suit was resolved entirely within state court. Though Daniel's suit was initially dismissed at the district level on traditional Section 230 grounds, she won on appeal in the Wisconsin Court of Appeals in 2018 before the Wisconsin Supreme Court reversed the decision the next year.

Daniel alleged that specific Armslist features, all relating to the management and display of user-generated content, resulted in the harms she experienced at the hands of Radcliffe Haughton. The features include the ability to search specifically for private sellers, the lack of registration requirements, and a failure to mandate waiting periods before users can sell arms to one another.[56] The suit contends that Armslist's failure to incorporate these features indicates a desire to facilitate illegal firearms sales.

The Wisconsin Court of Appeals, "applying a plain language interpretation to the Act," found that Section 230 did not shield Armslist from Daniel's claims. The court's ruling created a false dichotomy between claims treating Armslist as the publisher or speaker of information that users provided and claims relating to Armslist's functions as an editor or publisher. According to the court:

> It may be fair to characterize all of the operational and design features alleged by Daniel to be in some sense "content-based." However, in this respect, the content is not "information provided by another information content provider." Rather, it is content created by Armslist and there is no language

"Court-ordered changes to platform architecture would be most disruptive to end users, the greatest beneficiaries of intermediary liability protections."

> "If states do not require prospective gun buyers to wait between purchasing and receiving a firearm, websites that host gun advertisements cannot be expected to attempt to impose waiting periods."

in the Act immunizing Armslist from liability based on content that it creates.[57]

Armslist's editorial tools certainly belong to the platform, but the analysis should not end there. According to Daniel's complaint, Armslist's design features did not encourage or fail to prevent harm in the abstract. They failed to prevent a specific set of harms, stemming from Radcliffe Haughton's use of the platform. Thus, Daniel was not suing over the mere existence or nonexistence of certain features. She implicates them, or their absence, as they relate to specific pieces of user-generated speech that Armslist hosted but presumably did not help to create. This content, which Haughton posted using Armslist's tools, was causally integral to the harms she suffered.

In its reversal of the appellate court's decision, the Wisconsin Supreme Court recontextualizes Daniel's claims as ones that treat Armslist as the "publisher or speaker" of Haughton's speech.

> The complaint alleges that Armslist breached its duty of care by designing a website that could be used to facilitate illegal sales, failing to provide proper legal guidance to users, and failing to adequately screen unlawful content. Restated, it alleges that Armslist provided an online forum for third-party content and failed to adequately monitor that content. The duty Armslist is alleged to have violated derives from its role as a publisher of firearm advertisements. This is precisely the type of claim that is prohibited by § 230(c)(1), no matter how artfully pled.[58]

As such, Armslist's protection under Section 230 turns on whether it contributed to the illegality of the third-party content in question—that is, Radcliffe Haughton's "want to buy" ad and subsequent searches. If the processes to which Armslist subjected Haughton's ad and searches constituted "neutral assistance" (i.e., they processed his information as they would that of any other user and did not offer him special help in crafting his ad), they cannot be held liable for his speech or harms that stem therefrom. Outlining Armslist's features as implicated in Daniel's claims, the Wisconsin Supreme Court offered a definition of neutral tools as publishing processes that provide neutral assistance to users.

> The issue is whether Armslist was an information content provider with respect to Linn's advertisement. Armslist.com's provision of an advertising forum and the related search functions are all "neutral tools" that can be used for lawful purposes. Sales of firearms by private sellers are lawful in Wisconsin. Further, private sellers in Wisconsin are not required to conduct background checks, and private sales are not subject to any mandatory waiting period. Accordingly, the option to search for offers from private sellers is a tool that may be used for lawful purposes.[59]

Everything that Armslist's platform helped users do was perfectly legal. If the state of Wisconsin does not require prospective gun buyers to endure a waiting period between purchasing and receiving a firearm, websites that host gun advertisements cannot be expected to attempt to impose waiting periods on users. While Armslist could, hypothetically, require users to wait several days before contacting one another, such a requirement would handicap the site's usefulness.

More importantly, there is little reason to expect Armslist to go above and beyond the law in the name of safety, particularly when these demands would burden the exercise of constitutionally protected activity. Citing *Goddard v. Google Inc.*, a case concerning the mislabeling of paid ringtones as free in Google advertisements, the court notes that even if "a service provider knows that third parties are using such tools to create illegal content," this knowledge does not create a corresponding duty to prevent the feature's misuse.[60]

Neutral tools can usually be put to a wide range of both lawful and unlawful uses. In *Goddard*, Google's Keyword tool did "nothing more than provide options that advertisers may adopt or reject at their discretion."[61] The fact that Google both provided the keyword suggestion tool and knew that its advertising services were sometimes used in scams did not render it responsible for a criminal's willful selection of fraudulent product descriptions from a Google-suggested array. The *Daniel v. Armslist* court provides an inexhaustive list of other similarly protected neutral tools, linking their functionality and lawful uses.

> Examples of such neutral tools include a blank text box for users to describe what they are looking for in a roommate, *Roommates.com*, 521 F.3d at 1173, a rating system that allows consumers to award businesses between one and five stars and write reviews, *Kimzey v. Yelp! Inc.*, 836 F.3d 1263, 1270 (9th Cir. 2016), and a social media website that allows groups to create profile pages and invite members. *Klayman*, 753 F.3d at 1358. All of these features can be used for lawful purposes, so the CDA [Section 230] immunizes interactive computer service providers from liability when these neutral tools are used for unlawful purposes.[62]

Prohibiting the provision of these features, such as the ability to publish restaurant reviews, simply because they could be used to publish maliciously false reviews would deprive both diners and restaurants of the ability to benefit from a system of restaurant reviews. Likewise, the fact that some of Armslist's features, such as the ability to search only for in-state private sales, may benefit criminals unable to pass background checks does not diminish those features' value to lawful firearm buyers who wish to inspect a firearm before it is shipped to them or who live in areas with few licensed firearms dealers. Barring this search function to hamper criminals would deny it to lawful users as well. As such, because Armslist did not take part in creating the advertisement to which Haughton responded and because the tools provided via its website have lawful purposes, Section 230 precludes Daniel's claims. Daniel appealed her case to the U.S. Supreme Court, but as in *Herrick v. Grindr*, the nation's highest court declined to review the case.

Fair Housing Council of San Fernando Valley v. Roommates.com LLC established a firm distinction between providing neutral tools and participating in content creation. In *Herrick v. Grindr* and *Daniel v. Armslist*, courts simply applied this distinction to novel product liability and design negligence claims, maintaining a long-standing limit on liability. Drawing this line situates responsibility for misuse with the individual wrongdoer rather than blaming platforms and, in turn, collectively punishing lawful users. Erasing this distinction would imperil contemporary platforms that provide neutral tools while introducing regulatory uncertainty likely to stymie the development of new digital publishing services.

"Reasonable" Reform

While ultimately unsuccessful, these suits have inspired proposals for legislative reform. *Herrick v. Grindr* was once presented as a case that could change Section 230; some critics now see it as a reason to amend the statute.[63]

Efforts to condition Section 230's protections on platforms' implementation of "reasonable" content moderation are viewed as remedies to the rulings in *Herrick v. Grindr* and *Daniel v. Armslist*. Danielle Citron and Benjamin Wittes have proposed an amendment that would add a new stipulation to Section 230: providers of an "interactive computer service" would be required to take "reasonable steps to address unlawful uses of its service that clearly create serious harm to others" to avoid being treated as the "publisher or speaker" of their users' speech.[64]

In testimony before an October 2019 House Committee on Energy and Commerce hearing titled "Fostering a Healthier Internet to Protect Consumers," Citron presented Armslist's neutral publication and search tools

"Because Armslist did not take part in creating the advertisement to which Haughton responded and because the tools provided via its website have lawful purposes, Section 230 precludes Daniel's claims."

"Differing standards between courts might create a more restrictive standard as platforms endeavor to simultaneously comply with multiple understandings of 'reasonable.'"

as features intended for, rather than incidentally used by, criminals. She cast the *Daniel v. Armslist* ruling as a problem requiring a legislative solution.

> Extending the immunity from liability to platforms that deliberately encourage, facilitate, or refuse to remove illegal activity would seem absurd to the CDA's drafters. But even more absurd is immunizing from liability enterprises that connect sellers of deadly weapons with prohibited buyers for a cut of the profits. Armslist.com can hardly be said to "provide 'educational and informational resources' or contribute to 'the diversity of political discourse.'"[65]

Under this theory of liability, Armslist's potential for misuse undercuts its status as an "informational resource" that Americans can use to arrange Second Amendment–protected activity. Citron went on to offer a reasonable moderation requirement as a way to solve the issue.

> There is a broader, though balanced, legislative fix that Benjamin Wittes and I have proposed. Under our proposal, platforms would enjoy immunity from liability *if* they could show that their content-moderation practices writ large are reasonable.[66]

The imposition of such a requirement would replace the current neutral tool jurisprudence with a demand that platforms proactively police their tools for misuse. To moderate responsibly, platforms would have to continually update their services to reflect evolving judicial understandings of a vague standard. Proponents of this requirement offer its "inherently flexible" nature as a selling point, but it should instead be cause for concern.[67]

Requiring reasonable moderation would create a formal process for the sort of judicial redesign proposed in both *Herrick v. Grindr* and *Daniel v. Armslist*. Is litigation a good way to determine whether it is reasonable to allow friends to track each other's locations or to let strangers playing online video games speak to one another? Unlike platform moderation decisions, judicial standards of reasonable moderation would apply across the industry writ large. In the absence of countervailing privacy or speech requirements, conditioning Section 230 on reasonable moderation would incentivize platforms to prioritize greater moderation over conflicting user values. Indeed, it is far from certain that a platform attempting to govern speech in line with the First Amendment would be protected under a reasonable moderation standard. Differing standards of reasonableness between courts might create an effective standard more restrictive than the sum of its parts as platforms endeavor to simultaneously comply with multiple understandings of "reasonable."

Having a standard that requires platforms to balance free, even constitutionally protected, expression with the demands of reasonable moderation would open the door to the use of definitions of "reasonable moderation" that preclude disfavored forms of protected speech. Litigants in *Daniel v. Armslist* demanded that the platform limit communication between lawful private sellers. The architects of a reasonable moderation requirement seem to agree, casting the facilitation of communication necessary to arrange a private firearm sale as presumptively unreasonable.

Legislation requiring reasonable moderation that would exclude speech that might abet illegal activity amounts to a reinstatement of the "bad tendency test" via private platforms. This long-rejected First Amendment standard allowed government to restrict speech that had a "natural and probable tendency" to result in illegal behavior.[68] Under a reasonable moderation requirement, platforms would essentially be required to police speech and remove features deemed to have a propensity to produce illegal activity. Neglecting the long-standing distinction between the provision of speech tools and participation in speech, such a change would

place a new gauntlet of jawboned censorship between American speakers and American audiences.

More insidiously, some of the effects of a reasonable moderation requirement might be felt only as stagnation. Citron and Wittes predict that Omegle, a video chat platform that pairs users with random strangers, "would likely not be immune under such a standard."[69] How might speed dating in virtual reality or new forms of encrypted messaging fare under a standard that treats ungoverned interactions between individuals as unacceptably dangerous? If new means of one-to-one or one-to-many communication are considered innately irresponsible, a reasonable moderation requirement would preclude their creation in the first place. A legislative amendment to Section 230 would change the rules for all platforms, not just Grindr and Armslist. As such, the reform movement that *Herrick v. Grindr* and *Daniel v. Armslist* inspired poses a broader threat to Americans' access to digital publishing tools than either platform-specific lawsuit.

CONCLUSION

Compared to their analog cousins, digital neutral tools may seem easy to govern, but their sheer scale renders moderation difficult and forces tradeoffs between openness and effective enforcement. Although a pair of early intermediary liability cases, *Stratton Oakmont Inc. v. Prodigy Services Co.* and *Cubby Inc. v. CompuServe Inc.*, created perverse incentives for platform moderators, Congress fixed this problem with the passage of Section 230. This statutory speech protection prevents platforms from being treated as the publisher of user-generated content and was intended to ensure the availability and continued development of digital communications tools.

Despite often being derided as a protection for industry, Section 230 is effectively a protection for speakers—a product of the recognition that, without ready access to contemporary communications tools, Americans' speech rights would lose their vitality in the Internet Age. Far from being a unique shield, Section 230 sits comfortably within the First Amendment tradition of the press as a technology and shares similarities with other rights-enhancing statutes such as the Protection of Lawful Commerce in Arms Act. As such, recent product liability suits intended to circumvent Section 230's protections contravene the statute's purpose and threaten Americans' access to the tools upon which they increasingly rely.

Although digital publishing tools may be misused to malignant ends, Section 230 and an appreciation of platforms' importance to Americans' ability to exercise their speech rights preclude redesign via litigation as remedy. Product liability suits such as *Herrick v. Grindr* and *Daniel v. Armslist* ostensibly concern platform design features rather than hosted speech. However, their cited harms stem from some platform republication of user speech. As a result, in their attempts to circumvent Section 230, these suits' theories of content creation implausibly present neutral assistance as participation or encouragement.

As digital communication becomes even more central to American life, the disruptive potential of similar lawsuits will only increase. A second suit against Armslist in the style of *Daniel v. Armslist* has already been filed, and similar suits against Snapchat and Amazon are making their way through the courts. Legislative proposals to require reasonable moderation threaten to replace the neutral tool standard with an ongoing responsibility to police platform misuse without regard for the costs to speech. As these efforts advance, Americans' continued access to 21st-century means of expression will depend on a renewed appreciation of the link between intermediary liability protections and the availability of communicative tools that guided Section 230's creation two and a half decades ago.

"Legislative proposals to require reasonable moderation threaten to replace the neutral tool standard with an ongoing responsibility to police platform misuse."

NOTES

1. Shevaun Bryan, "Armed Teens Arrested at Metro Bank, Call Uber to Get Away," KFOR, updated February 9, 2019.

2. Gwern Branwen, "Silk Road 1: Theory & Practice," July 11, 2011.

3. Cyrus Farivar, "Judge Denies Silk Road's Demands to Dismiss Criminal Prosecution," *Ars Technica*, July 9, 2014.

4. Jack Nicas and Keith Collins, "How Apple's Apps Topped Rivals in the App Store It Controls," *New York Times*, September 9, 2019.

5. "Company Info," About Facebook, Facebook, https://about.fb.com/company-info/.

6. YouTube Team, "An Update on Our Commitment to Fight Terror Content Online," News & Events, YouTube Official Blog, October 17, 2017, https://youtube.googleblog.com/2017/08/an-update-on-our-commitment-to-fight.html.

7. Tarleton Gillespie, "Three Imperfect Solutions to the Problem of Scale," in *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (New Haven: Yale University Press, 2018), pp. 77–110.

8. See Justice Stevens's discussion of the use of credit cards as an age verification metric in *Reno v. ACLU*: "Using credit card possession as a surrogate for proof of age would impose costs on noncommercial Web sites that would require many of them to shut down. . . . Moreover, the imposition of such a requirement 'would completely bar adults who do not have a credit card and lack the resources to obtain one from accessing any blocked material,'" *(internal citations omitted), Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997) at 856.

9. Communications Act of 1934, 47 U.S.C. § 230 (1996).

10. Section 230 includes exceptions for federal criminal law, intellectual property governed by the Digital Millennium Copyright Act, and since the passage of SESTA/FOSTA (the combined Stop Enabling Sex Traffickers Act and Allow States and Victims to Fight Online Sex Trafficking Act), content that promotes or facilitates prostitution. As well, when providers take part in content creation, the resultant content cannot be considered "content created by another," so their republication does not receive the protection of Section 230. See *Fair Housing Council v. Roommates.com*, 521 F.3d 1157 (9th Cir. 2007).

11. Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Ithaca: Cornell University Press, 2019), pp. 26–30.

12. *Smith v. California*, 361 U.S. 147 (1959).

13. *Cubby Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).

14. Kosseff, *The Twenty-Six Words That Created the Internet*, p. 57.

15. *Stratton Oakmont Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. 1995).

16. *Stratton Oakmont Inc. v. Prodigy Services Co*.

17. *Auvil v. CBS "60 Minutes,"* 800 F. Supp. 928 (E.D. Wash. 1992) at 931.

18. *Auvil v. CBS "60 Minutes"* at 932.

19. Brent Skorup and Jennifer Huddleston, "The Erosion of Publisher Liability in American Law, Section 230, and the Future of Online Curation," Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, July 2019, p. 27. See also Julio Sharp-Wasserman, "Section 230(c)(1) of the Communications Decency Act and the Common Law of Defamation: A Convergence Thesis," *Columbia Science and Technology Law Review* 20, no. 1 (2018): 195–9.

20. Kosseff, *The Twenty-Six Words That Created the Internet*, p. 56.

21. *Reno v. American Civil Liberties Union*.

22. 47 U.S.C. § 230.

23. Taylor Hatmaker, "Nancy Pelosi Warns Tech Companies That Section 230 Is 'in Jeopardy,'" *TechCrunch*, April 12, 2019.

24. Makena Kelly, "Internet Giants Must Stay Unbiased to Keep Their Biggest Legal Shield, Senator Proposes," *The Verge*, June 19, 2019.

25. Allum Bokhari, "Bokhari: Eight Ways to Curb Google," *Breitbart*, July 23, 2019, https://www.breitbart.com/tech/2019/07/23/bokhari-seven-ways-to-curb-google/.

26. *Reno v. American Civil Liberties Union* at 870, "Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from

any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer. As the District Court found, 'the content of the Internet is as diverse as human thought.' We agree with its conclusion that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium."

27. Francis Robinson, "Technology and Religious Change: Islam and the Impact of Print," *Modern Asian Studies* 27, no. 1 (February 1993): 229–51.

28. David B. Sentelle, "Freedom of the Press: A Liberty for All or a Privilege for a Few?," *Cato Supreme Court Review 2013–2014*, pp. 15–34.

29. Eugene Volokh, "Freedom for the Press as an Industry, or for the Press as a Technology? From the Framing to Today," *University of Pennsylvania Law Review* 160, no. 2 (December 2011): 489–96.

30. Volokh, "Freedom for the Press as an Industry," p. 495.

31. *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964) at 266.

32. Congress passed the Securing the Protection of our Enduring and Established Constitutional Heritage Act, which prevents the enforcement of foreign libel judgements, in response to suits brought against American authors in foreign courts. Roy Greenslade, "Obama Seals Off US Journalists and Authors from Britain's Libel Laws," *The Guardian*, August 11, 2010.

33. Sen. Ted Cruz (R-TX), letter to Robert Lighthizer (U.S. Trade Representative), November 1, 2019, https://www.cruz.senate.gov/files/documents/2019.11.01_USTR%20Sec%20230%20LTR.pdf.

34. Protection of Lawful Commerce in Arms Act, 15 U.S.C., ch. 105.

35. David Kopel, "The Protection of Lawful Commerce in Arms Act: Facts and Policy," opinion, *The Washington Post*, May 24, 2016.

36. Eric Bradner, "Bernie Sanders Wants to 'Bring Us to the Middle' on Guns," CNN, July 5, 2015.

37. 15 U.S.C. § 7901.

38. Eric Goldman, "Why Section 230 Is Better Than the First Amendment," *Notre Dame Law Review* 95, no. 1 (November 2019): 33–46.

39. Petition for a Writ of Certiorari, Counsel for Petitioner, *Herrick v. Grindr LLC*, https://www.cagoldberglaw.com/wp-content/uploads/2019/08/HERRICK_SCOTUS.pdf.

40. Brief for Plaintiff-Appellant, *Herrick v. Grindr LLC*, pp. 2–5, https://epic.org/amicus/230/grindr/Herrick-v-Grindr-Appellant-Brief.pdf. My analysis is limited to Herrick's product liability claims, as they most clearly contravene the purpose of Section 230. Herrick also contended that Grindr somehow continued to provide his location to prospective sexual partners, even after he deleted the app. While he initially claimed that suitors visited his home and place of work, he expanded this claim in his Second Circuit Appeal. Here, he argued that his location information was linked to the impostor profile, allowing suitors to follow him everywhere he went. This is facially implausible. Even if Grindr were still collecting Herrick's locative information, there is no evidence to suggest that it would have been attached to the impostor account created by J.C. However, had Grindr provided Herrick's ex with his real-time location data for whatever reason, the information used in the harassing profile would have been provided by Grindr, obviating Grindr's protections under Section 230. See Cathy Gellis, "Herrick v. Grindr—The Section 230 Case That's Not What You've Heard," *Techdirt*, January 22, 2019.

41. *Herrick v. Grindr LLC*, No. 17-CV-932 (VEC), 2017 WL 744605 (S.D.N.Y. Feb. 24, 2017).

42. Brief for Plaintiff-Appellant, *Herrick v. Grindr*.

43. Brief for Plaintiff-Appellant, *Herrick v. Grindr*, p. 31.

44. Quentin Hardy, "VPNs Dissolve National Boundaries Online, for Work and Movie-Watching," *Bits* (blog), *New York Times*, February 8, 2015.

45. Brief for Plaintiff-Appellant, *Herrick v. Grindr*, p. 28.

46. *Herrick v. Grindr LLC*, 18-396 (2d Cir. 2019) at 6.

47. The court could have also relied upon *Carafano v. Metrosplash.com Inc.*, an early internet dating case with a remarkably similar fact pattern to *Herrick v. Grindr LLC*. Someone created a fake dating profile of actress Chase Masterson on the dating site Matchmaker, using it to direct harassers to her home. The Ninth Circuit examined the relationship between solicitation, presentation, and creation, finding that platform decisions to present user-generated content in one fashion or another do not constitute content creation. "Similarly, the fact that

Matchmaker classifies user characteristics into discrete categories and collects responses to specific essay questions does not transform Matchmaker into a 'developer' of the 'underlying misinformation.' . . . Matchmaker's decision to structure the information provided by users allows the company to offer additional features, such as 'matching' profiles with similar characteristics or highly structured searches based on combinations of multiple-choice questions. Without standardized, easily encoded answers, Matchmaker might not be able to offer these services and certainly not to the same degree." *Carafano v. Metrosplash.com Inc.*, 339 F.3d 1119 (9th Cir. 2003) at 11235.

48. *Fair Housing Council of San Fernando Valley v. Roommates.com LLC*, 521 F.3d 1157, 1168 (9th Cir. 2008) (en banc).

49. *Fair Housing Council of San Fernando Valley v. Roommates.com LLC* at 1174–75.

50. *Herrick v. Grindr LLC*, 18-396 (2d Cir. 2019) at 7.

51. Danielle Keats Citron, "Should We Reform Section 230?," American Enterprise Institute, streamed live on September 6, 2019, YouTube video, 1:27:54.

52. Citron, "Should We Reform Section 230?"

53. Armslist: Firearms Marketplace, https://www.armslist.com/.

54. Myra Sanchick and Meghan Dwyer, "Full Report from Azana Salon & Spa Mass Shooting Released," FOX6Now.com, March 1, 2013.

55. *Daniel v. Armslist LLC*, 2018 WL 1889123 (Wis. Ct. App. 2018) at 13.

56. *Daniel v. Armslist LLC*, 2018 WL 1889123 at 13–15.

57. *Daniel v. Armslist LLC*, 2018 WL 1889123 at 44.

58. *Daniel v. Armslist LLC*, 2019 WI 47 (Wis. 2019) at 51.

59. *Daniel v. Armslist LLC*, 2019 WI 47 at 37.

60. *Daniel v. Armslist LLC*, 2019 WI 47 at 29.

61. *Goddard v. Google Inc.*, 640 F. Supp. 2d 1193 (N.D. Calif. 2009) at 1198.

62. *Daniel v. Armslist LLC*, 2019 WI 47 at 33.

63. Tyler Kingkade and Davey Alba, "A Man Sent 1,000 Men Expecting Sex and Drugs to His Ex-Boyfriend Using Grindr, a Lawsuit Says," *Buzzfeed News*, January 10, 2019; and Carrie Goldberg, "Herrick v. Grindr: Why Section 230 of the Communications Decency Act Must Be Fixed," *Lawfare*, August 14, 2019.

64. Danielle Keats Citron and Mary Anne Franks, "The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform," Boston University School of Law Public Law Research Paper no. 20-8, February 1, 2020, pp. 21–22.

65. *Hearing on Fostering a Healthier Internet to Protect Consumers, Before the House Comm. on Energy and Commerce*, 118th Cong. 5 (2019) (written testimony of Daniel Keats Citron, professor of law, Boston University School of Law).

66. *Hearing on Fostering a Healthier Internet to Protect Consumers, Before the House Comm. on Energy and Commerce*, 118th Cong. 8 (2019) (written testimony of Danielle Keats Citron, professor of law, Boston University School of Law).

67. Neil Fried, "Instead of Crying Wolf on Section 230 Reform, Platforms Should Focus on the Predators Within," opinion, *The Hill*, July 29, 2020.

68. *Schaefer v. United States*, 251 U.S. 466 (1920) at 1.

69. Danielle Keats Citron and Benjamin Wittes, "The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity," *Fordham Law Review* 86, no. 2 (2017): 419, https://ir.lawnet.fordham.edu/flr/vol86/iss2/3.

CITATION

Duffield, Will. "Circumventing Section 230: Product Liability Lawsuits Threaten Internet Speech," Policy Analysis no. 906, Cato Institute, Washington, DC, January 26, 2021. https://doi.org/10.36009/PA.906.