18-396

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

MATTHEW HERRICK,

Appellee,

v.

GRINDR, LLC,

Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF APPELLANT AND URGING REVERSAL

Marc Rotenberg
Counsel of Record
Alan Butler
Natasha Babazadeh
Electronic Privacy
Information Center (EPIC)
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

May 31, 2018

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and 29(c) for Case No. 13-422 *amicus curiae* Electronic Privacy Information Center ("EPIC") states that it is a District of Columbia corporation with no parent corporation or publicly-held company with a 10 percent or greater ownership interest. EPIC is a non-profit, non-partisan corporation, organized under section 501(c)(3) of the Internal Revenue Code.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF AMICUS CURIAE[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC routinely participates as *amicus curiae* in cases about consumer privacy before the United States Supreme Court and federal circuit courts. *See, e.g.*, *Smith v. Facebook, Inc.*, No. 17-16206 (9th Cir. filed Sept. 25, 2017) (arguing that Facebook users do not consent to Facebook's collection of medical data from third-party websites); *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (arguing that the violation of a consumer's privacy rights under federal law constitutes an injury-in-fact sufficient to confer Article III standing); *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262 (3rd Cir. 2016) (arguing that unique persistent identifiers are "personally identifiable information" under the Video Privacy Protection Act); *Fraley v. Batman*, 638 Fed. App'x 594 (9th Cir. 2016) (arguing that Facebook's "Sponsored Stories" settlement was not fair or sufficient for class members); *Joffe v. Google, Inc.*, 746 F.3d 920 (9th Cir. 2013) (arguing that

[1] The parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

interception of Wi-Fi communications from home networks violated the federal Wiretap Act).

SUMMARY OF THE ARGUMENT[2]

Dating platform companies should be required to take down impersonating profiles when they fail to respond to egregious and abusive conduct which they knew about and which they facilitated. Grindr received many notifications about the harmful activity targeted at the Plaintiff. Grindr had the ability and the authority to terminate the fake profiles and to stop the abuse. Yet the commercial service did nothing. Grindr argues that § 230 of the Communications Decency Act, the "Good Samaritan" provision, provides the company absolute immunity from suit. But Grindr is not a Good Samaritan, and Congress never intended § 230 to protect this corporate irresponsibility.

Grindr is well aware of the abuse that can take place on its social platform. It has explicitly reserved the right to limit such activity in its Terms of Service. But Grindr also contends that it cannot be compelled to act when it fails to take action against users who cause harm to other users and violate the company's Terms of Service. That is not what Congress intended with section 230.

---

[2] EPIC would like to thank its Spring 2018 Clerk, Sara Wolovick, for her help in preparing this amicus brief.

ARGUMENT

When Congress passed the comprehensive Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56, it substantially overhauled the regulatory structure governing the cable, telephone, and broadcast industries. Congress added several provisions concerning the Internet, including "obscenity and violence" online.[3] Section 230 created "Good Samaritan" protections for certain online service providers who restricted "access to objectionable material." H.R. Rept. No. 104-458, at 194 (1996) (Conf. Rep.). Section 230 stated that "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." 47 U.S.C. § 230(c)(1). A specific purpose of Section 230 was to overrule *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995), and "any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material." H.R. Rept. No. 104-458, at 194 (1996) (Conf. Rep.). Congress also included significant findings and policy statements in Section 230 that help to elucidate its intended scope. *See* 47 U.S.C. §§ 230(a), (b).

[3] The sections in Title V of the Telecommunications Act are referred to as the "Communications Decency Act of 1996" ("CDA"). *See* 110 Stat. 133, *codified at* 47 U.S.C. § 609 note. Section 509 within the CDA amended Title II of the Communications Act of 1934 to add the new § 230 to 47 U.S.C.

Nothing in the text, findings, or history of § 230 indicates that Congress intended to prevent courts from protecting users who suffer abuse and harassment online. Congress made clear that it is the "policy of the United States" to "encourage the development of technologies which *maximize user control* over what information is received by individuals, families, and schools who use the Internet and other interactive computer services," *Id.* § 230(b)(3) (emphasis added), and to "ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and *harassment* by means of computer," *Id.* § 230(b)(5) (emphasis added).

The question is whether Section 230 allows internet platforms, such as Grindr, to ignore rampant abuse, harassment, and impersonation directed toward the users of its services. The § 230 immunity provision targets defamation claims against a "publisher or speaker," not abuse or harassment claims against a service provider.[4] Without an ability to force platforms to take down malicious fake profiles, victims may be subjected to ongoing psychological, social, and financial harm. In the physical world, potential liability and injunctive actions require

[4] The Supreme Court has never addressed the scope of immunity under the statute, but the Court has relied upon the findings and policy statements codified in § 230(b) when interpreting other provisions in the Communications Act. *See Nat'l Cable & Telecomm. Ass'n Inc. v. Gulf Power Co.*, 534 U.S. 327, 360 (2002) (determining scope of Pole Attachment Act); *Ashcroft v. ACLU*, 535 U.S. 564, 566 (2002) (evaluating constitutionality of Child Online Protection Act).

businesses and individuals to prevent abusive behavior. There is no justification for treating online platforms differently. As Professor Danielle Citron has explained:

> In physical space, a business that arranged private rooms for strangers to meet, knowing that sexual predators were using its service to meet kids, would have to do a great deal more than warn people to proceed "at their own peril" to avoid liability when bad things happened. A physical magazine devoted to publishing user-submitted malicious gossip about nonpublic figures would face a blizzard of lawsuits as false and privacy-invading materials harmed people's lives. And a company that knowingly allowed designated foreign terrorist groups to use their physical services would face all sorts of lawsuits from victims of terrorist attacks. Something is out of whack—and requires rethinking—when such activities are categorically immunized from liability merely because they happen online.

Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 Fordham L. Rev. 401, 403 (2017).

I. Online harassment is a significant threat facing Americans today.

The Internet has changed substantially since Congress passed the Telecommunications Act in 1996. Advanced social media platforms did not exist when Congress enacted the law. Today companies aggregate detailed profiles and make them available to people around the world. As Professor Citron has explained:

> The Internet extends the life of destructive posts. Harassing letters are eventually thrown away, and memories fade in time. The web, however, can make it impossible to forget about malicious posts. Search engines index content on the web and produce it instantaneously. Indexed posts have no built-in expiration date; neither

> does the suffering they case. Search engines produce results with links to destructive posts created years earlier.

Danielle Keats Citron, *Hate Crimes in Cyberspace* 4 (2014).

As of 2017, 41 percent of Americans have experienced online harassment and 62 percent consider it a critical concern. Monica Anderson, *Key Takeaways on How Americans View—and Experience—Online Harassment*, Pew Research Ctr. (Jul. 11, 2017).[5] Life online is often characterized by harassment in its varying forms, from "creat[ing] a layer of negativity that people must sift through" to "compromise[ing] users' privacy, forc[ing] them to choose when and where to participate online, or even pos[ing] a threat to their physical safety." Maeve Duggan, *Online Harassment 2017*, at 3 (2017).[6] Of the many forms of harassment, nearly one-in-five Americans have been subjected to severe harassment, which may include physical threats, harassment over an extended period, sexual harassment or stalking. *Id.* And about 80 percent of Americans believe that online service providers have a responsibility to intervene when harassment occurs. *Id*. at 4.

Online harassment can lead to psychological harm. Almost a third of Americans who have experienced harassment online subsequently experience

[5] http://www.pewresearch.org/fact-tank/2017/07/11/key-takeaways-online-harassment/.
[6] http://www.pewinternet.org/2017/07/11/online-harassment-2017/.

some form of mental or emotional distress as a result of the harassment. *Id.* at 20. One-fifth of Americans who have experienced online harassment have reported problems arising as a result of the harassment. *Id.* These problems include harm to relationships with friends and family, damage to reputation, harm to romantic relationships, problems with work and school, financial loss, and trouble finding work and housing. *Id.*; *see also* Darrin Giglio, *The Psychological Effects of Cyber Bullying* (2017).[7] Online harassment can also inhibit speech. *See* PEN America, *Online Harassment Field Manual* (2018);[8] *see also* Erin Bartnett, *PEN America's New Guide Recognizes Online Harassment as a Threat to Free Speech*, Electric Lit. (Apr. 20, 2018).[9] Online users who witness harassment "may feel anxious or unsafe about their own interactions or participation online, and many are concerned that widespread harassment contributes to an environment in which people are scared or unwilling to speak freely for fear of retribution." Duggan, *supra*, at 35. More than a quarter of Americans have decided against posting something online after witnessing online harassment of third parties. *Id.* at 36. Almost half of American adults have taken measures in response to witnessing

[7] https://pvteyes.com/the-psychological-effects-of-cyber-bullying/.
[8] https://onlineharassmentfieldmanual.pen.org/.
[9] https://electricliterature.com/pen-america-s-new-guide-recognizes-online-harassment-as-a-threat-to-free-speech-8dbad8a19ea8.

online harassment, including refraining from posting, changing online information provided, or completely stopping use of the platform altogether. *Id.*

Under the lower court's interpretation of § 230, online platforms bear no responsibility for the harassment and abuse that their systems enable. If they chose not to respond to the exposure of personal information or intimate images, to threats of violence, to verbal and psychological abuse, there is nothing a victim can do to intervene. But Congress never intended § 230 to create such a system.

II. Social media companies know that their platforms enable abuse, and they assert authority to limit harassing behavior and to remove offending users.

Most, if not all, social media platforms recognize that their systems can facilitate harassment and abuse, and they prohibit such behavior and retain the right to block it. Platforms prohibit behavior such as impersonating individuals, stalking, harassing, abusing, defaming, threatening, and violating the privacy of other users, and disclosing the location or personal information of users without consent. These platforms explicitly retain the right to control such abusive behavior and prohibit the misuse of their systems. *See, e.g.,* OkCupid, *Terms & Conditions* (2018) (users must agree that they "shall not under any circumstances harass or make mischief against any other user of the Website.");[10] Tinder, *Terms of Use* (2018) (users must agree not to "bully, 'stalk,' intimidate, assault, harass,

[10] https://www.okcupid.com/legal/terms.

mistreat or defame any person," or "impersonate any person or entity or post any images of another person without his or her permission");[11] Match.com, *Terms of Use Agreement* (2017) (users "may not post…any offensive, inaccurate, abusive, obscene, profane, sexually oriented, threatening, intimidating, harassing, rude, vulgar, derogatory, sexist, defamatory, insulting, racially offensive, or illegal material, or any material that infringes or violates another person's rights");[12] Bumble, *Terms & Conditions* (2018) ("impose[s] restrictions on certain content which contains language or imagery which could be deemed offensive or is likely to harass" or "is abusive, insulting or threatening" or "shows another person which was created or distributed without that person's consent.").[13]

Grindr similarly prohibits users from impersonating individuals and from using its services to stalk, harass, abuse, defame, threaten, violate the privacy of other users, or disclose the location or personal information of other users without consent. Grindr, *Terms and Condition of Service* (2018).[14] In an instance where a user violates Grindr's terms of service, Grindr informs users it may ban accounts or request users to delete content. *Id.* But even though the platform has granted itself broad power to control and moderate its platform, Grindr has refused to

[11] https://www.gotinder.com/terms/us-2018-05-09.
[12] https://www.match.com/registration/membagr.aspx.
[13] https://bumble.com/terms.
[14] https://www.grindr.com/app/terms-of-service/?lang=en.

enforce its own policies. This goes against industry standards, and it is not the "Good Samaritan" behavior that Congress sought to incentivize in § 230, quite the opposite.

Grindr appears to stand alone in its refusal to police abuse. Tinder, OkCupid, Match.com, and Bumble all encourage its users to proactively report abusive behavior and fraudulent profiles. For example, OkCupid provides:

> If you believe that any user of this Website is harassing you or is otherwise using personal information about you for unlawful purposes, we encourage you to first inform local law enforcement authorities and then contact us via The Feedback Form so that we may take appropriate action to block further use of the Website by any user who is using this Website and information obtained from it for improper purposes.

OkCupid, *Terms & Conditions*. The company also provides a link to a 'feedback form' and directs users to the appropriate location to file a report. *See* OkCupid, *Support Feedback* (2018).[15] Tinder similarly requests that users report anyone engaging in offensive behavior. On its Safety Tips page, Tinder states to "please report anyone who violates our terms of use," which includes "[u]sers sending harassing or offensive messages," "[u]sers behaving inappropriately after meeting in person," and "[f]raudulent registration or profiles." Tinder, *Safety Tips* (2018).[16]

Match.com similarly provides a link for users to "report anyone who violates

[15] https://www.okcupid.com/feedback.
[16] https://www.gotinder.com/safety.

[its] terms of use." Match.com, *How to Date Safely* (2018).[17] The link directs users to a page that specifically addresses profile integrity, stating that Match.com "strive[s] to present only profiles of real people" and "[a]ll profiles submitted to Match.com go through an approval process," but also encourages users "to improve the overall Match.com experience" by reporting offensive behavior. Match.com, *Protecting Member Integrity on Match.com* (2018).[18] The platform has a specific team tasked with ensuring the "integrity" of user profiles:

> If you receive an inappropriate email or see a profile that seems suspicious in any way, please notify us. You can do this from any profile page or from any email received. This information goes directly to and is reviewed by our Member Integrity Team. If you want to report someone and need to locate the member again, search by the user name, then report your concern from the member's profile.

Id. Match.com also promises that any "fraudulent profile" will "be blocked from the site." *Id.* Bumble informs users to "report any abuse or complain about Member Content by contacting [them], outlining the abuse and/or complaint." Bumble, *Terms & Conditions* (2018). Also, Bumble provides an alternative method by enabling users to "report a user directly from a profile or in chat by clicking the 'Block & Report' link." *Id.*

Instead of following these industry standards to protect users from abuse, Grindr appears to do nothing. The platform does not encourage users to report

[17] https://www.match.com/help.safetytips.aspx.
[18] https://www.match.com/blocking/pu_abuseinfo.aspx?hdr=pop&lid=80.

offensive behavior. Grindr provides no link or mechanism for users to file complaints or to flag abusive behavior. Grindr does allow a user to block and report another user, but only provides a drop-down menu with select few concerns to choose from. Grindr, *Blocking and Reporting Users* (2018).[19] In a survey on Grindr's website, less than half of Grindr users found Grindr's webpage on blocking and reporting users actually helpful. *Id.*

Yet even as it ignores user complaints about abuse and fails to provide reasonable protection mechanisms, Grindr retains ultimate control over its platform. It could clearly take down an offending profile or block a user if it chose to do so. The Grindr agreement specifically states that the company may "delete [users'] submissions" and "ban [users'] account[s] . . . at any time for any reason, or no reason whatsoever." Grindr, *Terms and Conditions of Service*. Also, "any violations of the Guidelines or th[e] Agreement" can lead to user accounts "being banned" or access being terminated. *Id.*

Other platforms provide for meaningful control over user profiles. Match.com asserts that it may "terminate or suspend [user] subscription[s] and/or membership in the Service at any time" with a violation of the User Agreement. Match.com, *Terms of Use Agreement*. Tinder also alleges that it "reserves the right

[19] https://help.grindr.com/hc/en-us/articles/217763127-Blocking-and-Reporting-Users.

to review and remove Content that violates" its User Agreement. Tinder, *Terms of Use* (2018). OkCupid asserts that it "reserves the right, at its sole discretion, to deny further or continuing access to the Website to any visitor, including, without limitation, any user that OkCupid determines has violated any aspect of the[] Terms of Use." OkCupid, *Terms & Conditions*. It also reserves the right "to seek and obtain any other remedies available to it pursuant to any applicable laws and regulations or at equity as a result" of any violations. *Id.* And last, Bumble "reserve[s] the right . . . to terminate or suspend any Account, or make use of any operational, technological, legal or other means available to enforce the Terms (including without limitation blocking specific IP addresses), at any time without liability and without the need to give you prior notice." Bumble, *Terms & Conditions*. But unlike Grindr, these other platforms actually provide mechanisms for their users to flag abuse and to trigger action that would protect the users.

This power structure underscores the need for accountability when a platform refuses to respond to repeated notifications of abuse. There is no question that Grindr could easily prevent the abusive and harassing conduct by blocking the fake profiles and removing the Plaintiff's name and personal information. Grindr also asserts that it can suspend or block an account "at any time." Grindr, *Terms and Conditions of Service*. Yet when a user alerts the company about a fake profile actively being used to harm and harass them, the company chooses to do nothing

and argues that it cannot be held to account for that decision. Such an interpretation of § 230 would do nothing to "ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." 47 U.S.C. § 230(b)(5). The stated goal of the law is being undermined by the very company that argues that immunity should be granted in its favor. That cannot be what Congress intended.

III. The lower court's decision is contrary to the "Good Samaritan" provision in section 230.

This Court should not hold that a company is shielded under § 230 from all liability for abuse and harassment carried out on its platform. Such a broad liability protection would remove a key incentive for conducting oversight of user misconduct and would undercut the core purpose of § 230. Congress enacted the law to protect blocking and screening of offensive material by "Good Samaritans," and to promote the Internet as a source "of educational and informational resources," not to give platforms carte blanche to ignore harassment and abuse. *See* 47 U.S.C. §§ 230(a)(1), (b)(1), (c)(1).

A. Congress created the § 230 safe harbor to encourage internet service providers to police their platforms.

Congress intended § 230 "to encourage service providers to self-regulate the dissemination of offensive material over their services." *Zeran v. America Online*, 129 F.3d 327, 331 (4th Cir. 1997). The concern that gave rise to the amendment

was created by conflicting outcomes in two cases: one by the Southern District of New York in *Cubby, Inc. v. CompuServe*, 776 F. Supp. 135 (S.D.N.Y. 1991) and another by the New York trial court in *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995). In *CompuServe*, plaintiffs sued an "on-line general information service" for defamatory comments made by a columnist on its platform. 776 F. Supp. at 137. The court held that CompuServe was not liable because it had acted as a mere "distributor," having neither reviewed any of the column before it was posted nor had knowledge of its contents. *Id*. at 141. The *CompuServe* decision preserved the traditional distributor-publisher distinction that had applied to print media, but that distinction became more complicated as online platforms increasingly moderated their forums.

In *Stratton Oakmont*, plaintiffs sued an interactive computer service for defamatory comments made by a third party on a bulletin board. 23 Media L. Rep. 1794. Unlike the court in *CompuServe*, the court in *Stratton Oakmont* found that the service exercised editorial control and could therefore be liable for defamation. *Id.* Congress feared that the outcome in *Stratton Oakmont* would deter service providers from taking any steps to censor offensive material posted online. Congress therefore enacted § 230 "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."

47 U.S.C. § 230(b)(4). Representatives Christopher Cox and Ron Wyden first introduced § 230 as an amendment to the Telecommunications Act, expressly to protect "Good Samaritan" service providers who screened offensive material. H.R. Rep. No. 104-223, at 3, 14 (1995). Members of the House Judiciary Committee, including Representative Bob Goodlatte, echoed this view of the provision when it was introduced:

> Currently, however, there is a tremendous disincentive for online service providers to create family friendly services by detecting and removing objectionable content. These providers face the risk of increased liability where they take reasonable steps to police their systems. A New York judge recently sent the online services the message to stop policing by ruling that Prodigy was subject to a $200 million libel suit simply because it did exercise some control over profanity and indecent material.

141 Cong. Rec. 22,047. The House Rules Committee had previously described the purpose of the amendment as "protecting from liability those providers and users seeking to clean up the Internet." H.R. Rep. No. 104-223, at 3.

Nothing in the text, structure, or history of § 230 indicates that it should provide blanket immunity to service providers that do nothing to respond to repeated complaints about abuse and harassment on their platforms, and thereby negligently cause harm to innocent individuals. Protecting providers who fail to engage in any form of self-regulation is "antithetical" to the intent of the statute. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. Rev. 61, 116 n. 377 (2009).

Commentators have noted that the core purpose of the law was to protect users, not to put them at risk:

> Development of technologies that "maximize user control over what information is received" by Internet users, as well as the "vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, talking and harassment by means of computer." In other words, the law [wa]s intended to promote and protect the values of privacy, security and liberty alongside the values of open discourse.

Mary Anne Franks, *The Lawless Internet? Myths and Misconceptions About CDA Section 230*, Huffington Post (Feb. 17, 2014);[20] *see also* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 Harv. L. Rev. 1598, 1605–09 (2018).

The Supreme Court has yet to weigh in on the scope and meaning of § 230, but state and lower federal courts have reached a "near-universal agreement" that the provision should "not be construed grudgingly." *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 18 (1st Cir. 2016), *cert. denied*, 137 S. Ct. 622 (2017); *see also, e.g., Jones v. Dirty World Entm't Recordings LLC*, 755 F.3d 398, 406 (6th Cir. 2014); *Klayman v. Zuckerberg*, 753 F.3d 1354,1358 (D.C. Cir. 2014); *Doe v. MySpace, Inc.*, 528 F.3d 415, 418 (5th Cir. 2008); *Universal Commc'n Sys., Inc. v. Lycos, Inc.*, 478 F.3d 413, 419 (1st Cir. 2007); *Almeida v. Amazon.com,*

[20] http://www.huffingtonpost.com/mary-anne-franks/section-230-the-lawless-internet_b_4455090.html.

Inc., 456 F.3d 1316, 1321–22 (11th Cir. 2006); *Carafano v. Metrosplash.com, I*nc., 339 F.3d 1119, 1123 (9th Cir. 2003).

However, courts have also typically granted § 230 immunity to providers that actually engage in reasonable content moderation. The Seventh Circuit emphasized that it would be unreasonable to extend the immunity to providers that refuse reasonable requests to take down harmful content:

> As precautions are costly, not only in direct outlay but also in lost revenue from the filtered customers, ISPs may be expected to take the do-nothing option and enjoy immunity under § 230(c)(1). Yet § 230(c)—which is, recall, part of the "communications Decency Act"—bears the title "Protection for 'Good Samaritan' blocking and screening of offensive material", hardly an apt description if its principal effect is to induce ISPs to do nothing about the distribution of indecent and offensive materials via their services. Why should a law designed to eliminate ISPs liability to the creators of offensive material end up defeating claims by the victims of tortious or criminal conduct?

Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 670 (7th Cir. 2008). The immunity provision was purposefully enacted to incentivize proactive moderation by removing the threat of liability, not to shield those who refuse to engage in any form of regulation of platform policies.

The Ninth Circuit has similarly emphasized the gravity and dire implications of a broad interpretation of § 230. The court has found that the law was "not meant to create a lawless no-man's-land on the Internet." *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1164 (9th Cir. 2008). The Ninth Circuit emphasized:

> The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant-perhaps the preeminent-means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability.

Id. at n.15. In other words, a broad interpretation of § 230 immunity contradicts the policy objectives laid out in the statute. It neither "promote[s]" the internet as a platform for "educational and informational resources" nor encourages the "Good Samaritan" behavior of platforms that Congress sought to protect.

Much has changed with the Internet since § 230 was enacted. Technology companies have only grown "larger, more powerful, and less vulnerable than were the nascent online service providers of two decades ago." Citron & Wittes, *supra*, at 411. The internet "has outgrown its swaddling clothes and no longer needs to be so gently coddled." *Roommates.com*, 521 F.3d at 1175 n.39. Congress would not have imagined that the immunity it created for small bulletin board services who engaged in reasonable content moderation would shield enormous corporations from responsibility for the damage their platforms enable. *See also Algorithms: How Companies' Decisions About Data and Content Impact Consumers: Hearing Before the Subcomm. on Digital Commerce & Consumer Protection of the H. Comm. on Energy & Commerce*, 115th Cong. 15 (2017) (statement of Frank

Pasquale, Professor of Law, University of Maryland) (discussing the danger and "collateral consequences" of expanding § 230 immunity). Because the statutory text does not strictly define what it means to "be treated as the publisher or speaker" of information, this Court should construe the provision narrowly and consistent with its purpose. This Court should not grant to Bad Samaritans the protections that Congress intended to provide to Good Samaritans.

B. The lower court's broad interpretation of § 230 immunity would not advance the speech-promoting policy of the statute.

The lower court's broad interpretation of § 230 immunity would neither "promote the continued development of the internet" nor "preserve the vibrant and competitive free market" for educational and informational resources that the internet can enable. Such broad immunity would likely inhibit free speech. *See* Klonick, *supra*, at 1607-08 (noting that the Fourth Circuit in *Zeran* interpreted the dual congressional purposes of § 230 as (1) overturning *Stratton Oakmont* by providing protections for Good Samaritans, and (2) as a free speech protection for users meant "to encourage the unfettered and unregulated development of free speech on the Internet, and to promote the development of e-commerce.").

Section 230 was enacted to protect providers of bulletin board systems that enabled users to post and express their opinions while still engaging in reasonable content moderation. However, many modern platforms do not substantially promote free expression of internet users. Take, for example, Uber and Airbnb, a

transportation service and a real-estate rental service, respectively. These platforms have little to no impact on free speech because their business model aims to promote transportation and accommodations, as opposed to providing spaces to encourage speech. *See* Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 Colum. L. Rev. 1623 (2017). Despite their clear commercial purpose, businesses have attempted to claim § 230 immunity for such services. *See, e.g., Inman v. Technicolor USA, Inc.*, No. 11-666, 2011 WL 5829024, at *7 (W.D. Pa. Nov. 18, 2011) (holding that § 230 immunizes eBay from liability for one user's purchase of vacuum tubes from a third party that later caused mercury poisoning).

Focusing only on the interests of the platforms "gives an irrational degree of free speech benefit to harassers and scofflaws but ignores important free speech costs to victims." Citron & Wittes, *supra*, at 420. Also, "[a]n environment of perfect impunity for intermediaries that facilitate online abuse is not an obvious win for free speech if the result is that the harassers speak unhindered and the harassed retreat in fear offline." *Id*. Grindr's failure to regulate offensive material inhibits a victim's ability to engage on its platform and enables harassers to maximize offensive content. Because of the abuse he suffered, the Plaintiff no longer uses the platform. Am. Compl. ¶ 48, JA-65. During this period, Grindr selected and directed over a thousand strangers wanting sex—sometimes violently

insisting on it—to Herrick's home and workplace when it should have instead prevented or, at least, mitigated the impact and harm, especially after it had been repeatedly notified. Am. Compl. ¶ 49, JA-65.

Interpreting § 230 as providing blanket immunity to online service providers that ignore their Good Samaritan obligations grants such providers a license to disregard illegal activity, or even reward that activity directly or indirectly. And the resulting harassment and abuse creates a chilling effect for victims and other users, limiting free speech and discouraging user control. Users may reasonably fear that continued engagement on these platforms will cause harm, and they will be forced to disengage. This is simply not what Congress intended when it enacted § 230.

CONCLUSION

Amici curiae EPIC et al. respectfully request this Court rule for the Appellants and reverse the lower court decision.

Respectfully submitted,

/S/ MARC ROTENBERG

Marc Rotenberg
Counsel of Record
Alan Butler
Natasha Babazadeh
Electronic Privacy
Information Center (EPIC)
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140
amicus@epic.org

May 31, 2018

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 7,000 words of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(B). This brief contains 5,117 words, excluding the parts exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word Mac in 14 point Times New Roman style.

Dated: May 31, 2018

/S/ MARC ROTENBERG_

CERTIFICATE OF SERVICE

I hereby certify that on this 31st day of May 2018, the foregoing Brief of *Amicus Curiae* was electronically filed with the Clerk of the Court, and thereby served upon counsel for the parties *via* electronic mail.

Dated: May 31, 2018

/S/ MARC ROTENBERG