No. 19-153

IN THE

Supreme Court of the United States

YASMEEN DANIEL, INDIVIDUALLY, AND AS SPECIAL ADMINISTRATOR OF THE ESTATE OF ZINA DANIEL HAUGHTON,

PETITIONER,

V.

ARMSLIST, LLC, AN OKLAHOMA LIMITED LIABILITY COMPANY, BRIAN MANCINI AND JONATHAN GIBBON,

RESPONDENTS.

ON PETITION FOR A WRIT OF CERTIORARI TO THE SUPREME COURT OF WISCONSIN

BRIEF *AMICUS CURIAE* OF THE CYBER CIVIL RIGHTS INITIATIVE AND LEGAL SCHOLARS IN SUPPORT OF PETITIONERS

Jeffrey A. Mandell
Counsel of Record
STAFFORD ROSENBAUM LLP
222 W. Washington Ave., #900
P.O. Box 1784
Madison, WI 53701-1784
jmandell@staffordlaw.com
608.256.0226

Counsel for Amici Curiae *The Cyber Civil Rights Initiative, Ann Bartow, Danielle Keats Citron, Dr. Mary Anne Franks, Woodrow Hartzog, Frank Pasquale, Neil Richards, Dr. Olivier Sylvain, and Dr. Ari Ezra Waldman*

August 30, 2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

Statutes

Other Authorities

INTEREST OF AMICI CURIAE

The Cyber Civil Rights Initiative ("CCRI") and the undersigned law professors submit this brief as amici curiae in support of Plaintiff-Appellant Yasmeen Daniel's petition for certiorari.[1] Amicus CCRI is a nonprofit organization dedicated to the protection of civil rights in the digital era. CCRI is particularly concerned with abuses of technology that disproportionately impact vulnerable groups. CCRI works with tech-industry leaders, policymakers, courts, and law enforcement to address online abuses including "doxing" (the release of private information for the purpose of harassment), "revenge porn" (a specific form of doxing that involves the unauthorized disclosure of private, sexually explicit imagery), and defamation. CCRI provides support to victims of online abuse through its crisis helpline, network of pro bono legal services, and guidelines for navigating the reporting and removal procedures of online platforms. CCRI also works with social media and technology

[1] Counsel of record for the parties received timely notice of amici's intent to file, and this brief is submitted with their consent. Amici state that no party's counsel authored this brief in whole or in part; no party's counsel contributed money that was intended to fund preparing or submitting the brief; and no person—other than amici—contributed money to fund preparing or submitting the brief.

companies to develop policies to prevent misuses of their services and platforms.

The legal scholar amici have deep expertise in this area of the law and have written extensively about Section 230 and intermediary liability. Three are members of CCRI's board of directors: President and Legislative and Tech Policy Director Dr. Mary Anne Franks, a First Amendment expert and professor of law at the University of Miami Law School; Vice-President Danielle Keats Citron, a privacy expert and professor of law at Boston University School of Law; and Dr. Ari Ezra Waldman, Professor of Law and Director of the Innovation Center for Law and Technology at New York Law School. They are joined in this brief by Ann Bartow, professor of law at the University of New Hampshire School of Law, Woodrow Hartzog, professor of law and computer science at the Northeastern University School of Law, Frank Pasquale, Piper & Marbury Professor of Law at the University of Maryland School of Law, Neil Richards, Koch Distinguished Professor of Law at Washington University in St. Louis School of Law, and Dr. Olivier Sylvain, professor of law at Fordham Law School.

INTRODUCTION AND SUMMARY OF ARGUMENT

In the physical world, it is indisputable that third parties can sometimes be held liable for other people's actions. Many harmful acts are only possible with the participation of multiple actors with various motivations. The doctrines of aiding and abetting, complicity, and conspiracy all reflect the insight that third parties who assist, encourage, ignore, or contribute to the illegal actions of another person can and should be held responsible for their contributions to the concomitant harms. It is a central tenet of tort law that the possibility of such liability incentivizes individuals and industries to act responsibly and reasonably. Conversely, grants of immunity from such liability risk encouraging negligent and reckless behavior.

The question raised by this case is whether these well-understood and settled understandings of liability and immunity simply do not apply to the Internet. That is the necessary consequence of the maximalist interpretation of Section 230 of the Communications Decency Act of 1996 by the Wisconsin Supreme Court. By contrast, courts properly mindful of Section 230's text, goals, and history have interpreted the law to modify, rather than obliterate, fundamental concepts of liability and immunity for online activity.

The argument advanced in this amicus brief has four parts. Part I provides perspective on how courts' widely divergent interpretations of Section 230 of the Communications Decency Act of 1996 have created general confusion and undermined public welfare. Part II demonstrates how the Wisconsin Supreme Court's maximalist interpretation of Section 230 not only violates the text and purpose of the statute, but also distorts First Amendment doctrine and hinders the operation of the free market. Part III explains why it is not unduly burdensome for intermediaries to engage in responsible design of their platforms and services. Part IV describes how an overly expansive interpretation of Section 230 particularly endangers the welfare and civil liberties of vulnerable groups, including domestic violence victims.

Without clear guidance from this Court as to the proper scope and application of Section 230, individuals and industries can continue to evade liability for negligent and reckless practices simply by moving them online. Accordingly, this Court's review is urgently needed to ensure that Section 230 is used to uphold, rather than erode, the rule of law online.

ARGUMENT

I. The extreme variation in the way that courts interpret Section 230 has created widespread confusion and uncertainty about what constitutes lawful and unlawful behavior on the Internet.

As of July 2019, more than 4 billion people–56% of the global population–were active Internet users. J. Clement, *Global digital population as of July 2019 (in millions)*, Statista (Aug. 9, 2019).[2] The United States has the third-highest number of Internet users in the world: 293 million users, or 87% of its population. J. Clement, *Internet usage in the United States - Statistics & Facts*, Statista (Aug. 20, 2019).[3] People use the Internet not only to communicate, including via email, text message, and social media networks, but also to buy and sell merchandise, deposit checks, make restaurant reservations, watch videos, read books, stream music, and look for employment. J. Clement, *Most popular online activities of adult internet users in the United States as of November 2017*, Statista (Nov. 7,

---

[2] https://www.statista.com/statistics/617136/digital-population-worldwide/.

[3] https://www.statista.com/topics/2237/internet-usage-in-the-united-states/.

2018).[4] Today, there is almost no aspect of most people's daily lives that does not have an online component. "Cyberspace" is no longer a realm distinct or separable from physical space; the offline and online worlds are inextricably linked.

However, the online and offline worlds are governed by very different rules. For better or for worse, Congress in 1996 decided that the law of the Internet should depart significantly from the law of real space. Much of Congress's early attempt to regulate the Internet through the Communications Decency Act was struck down by this Court for violating the First Amendment (*see Reno v. Am. Civil Liberties Union*, 521 U.S. 844 (1997)), but Section 230 remained. Section 230, at its most basic level, is a limitation of what legal liability can be imposed for Internet activity. More specifically, it limits when and how online intermediaries ("interactive computer services") can be held accountable for the actions of those who use their platforms and services.

Section 230 has been called the "Magna Carta of the Internet," (Noa Yachot, *The 'Magna Carta' of Cyberspace Turns 20: An Interview With the ACLU Lawyer Who Helped Save the Internet*, ACLU (June

[4] https://www.statista.com/statistics/183910/internet-activities-of-us-users/.

23, 2017)[5]), and the "cornerstone of Internet freedom." Berin Szoka, *Section 230: The Cornerstone of Internet Freedom*, Tech Liberation (Aug. 18, 2009)[6]; *see also* Elizabeth Nolan Brown, *Section 230 Is the Internet's First Amendment. Now Both Republicans and Democrats Want To Take It Away*, Reason (July 29, 2019) ("[T]he entire suite of products we think of as the internet—search engines, social media, online publications with comments sections, Wikis, private message boards, matchmaking apps, job search sites, consumer review tools, digital marketplaces, Airbnb, cloud storage companies, podcast distributors, app stores, GIF clearinghouses, crowdsourced funding platforms, chat tools, email newsletters, online classifieds, video sharing venues, and the vast majority of what makes up our day-to-day digital experience—have benefited from the protections offered by Section 230.").[7] It has also been called "the one law that's the cause of everything good and terrible about the Internet." Paul Blumenthal, *The*

---

[5] https://www.aclu.org/blog/free-speech/internet-speech/magna-carta-cyberspace-turns-20-interview-aclu-lawyer-who-helped.

[6] https://techliberation.com/2009/08/18/section-230-the-cornerstone-of-internet-freedom/.

[7] https://reason.com/2019/07/29/section-230-is-the-internets-first-amendment-now-both-republicans-and-democrats-want-to-take-it-away/.

One Law That's the Cause of Everything Good and Terrible About the Internet, Huffington Post (Aug. 6, 2018).[8]

Given Section 230's extraordinary influence, it is not surprising that it generates controversy. The law is both vigorously praised and criticized; calls to amend the law have increased in the last few years and have been met with vociferous opposition. Cristiano Limo, *How a widening political rift over online liability is splitting Washington*, Politico (July 9, 2019).[9] Professor Jeff Kosseff, author of *The Twenty-Six Words That Created the Internet,* a book about Section 230, observed in August 2019 that "[t]here is definitely more attention being paid to Section 230 than at any time in its history." Daisuke Wakabayashi, *Legal Shield for Websites Rattles Under Onslaught of Hate Speech*, N.Y. Times (Aug. 6, 2019).[10]

Much of this attention is deeply confused. A number of high-profile politicians have claimed, for example, that the law requires online intermediaries to be "neutral platforms" or lose their immunity,

---

[8] https://www.huffpost.com/entry/online-harassment-section-230_n_5b4f5cc1e4b0de86f488df86.

[9] https://www.politico.com/story/2019/07/09/online-industry-immunity-section-230-1552241.

[10] https://www.nytimes.com/2019/08/06/technology/section-230-hate-speech.html.

(Sarah Jeong, *Politicians Want to Change the Internet's Most Important Law. They Should Read It First*, N.Y. Times (July 26, 2019)[11]), a claim that finds no support in either the text of the statute or case law interpreting it. Jeff Kosseff, *Correcting a Persistent Myth About the Law that Created the Internet*, The Regulatory Review (July 15, 2019).[12] In another example, a *New York Times* headline that referred to Section 230 as protecting "hate speech" generated such intense criticism that the newspaper changed the headline and issued a correction the next day. *Corrections: August 7, 2019*, N.Y. Times.[13]

While some of the claims made about Section 230 can be ascribed to political strategizing, another reason for the widespread confusion about what Section 230 does and does not do is that, as the Petition for Writ of Certiorari describes in detail (*see* pages 14–29), courts have interpreted the law in wildly divergent ways.

---

[11] https://www.nytimes.com/2019/07/26/opinion/section-230-political-neutrality.html.

[12] https://www.theregreview.org/2019/07/15/kosseff-correcting-persistent-myth-about-law-that-created-the-internet/.

[13] https://www.nytimes.com/2019/08/06/pageoneplus/corrections-august-7-2019.html.

At one extreme is the view that the law provides near-total immunity to online intermediaries with regard to their users' conduct. In the Fourth Circuit's expansive view, for example, "§ 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third party user of the service." *Zeran v. Am. Online*, 129 F.3d 327, 330 (4th Cir. 1997). Other courts have taken a much narrower approach, maintaining that Section 230 provides no "immunity" at all, but only "limits who may be called the publisher of information that appears online." *City of Chi. v. Stubhub!, Inc.*, 624 F.3d 363, 366 (7th Cir. 2010). Courts furthermore disagree about what constitutes impermissible treatment as a "publisher or speaker"; how to define an "information content provider"; what it means to "develop" content; and whether website design counts as "content." (Pet. at 14–29.)

Such variation in how Section 230 has been interpreted makes it difficult for the wide array of online intermediaries, as well as the billions of Internet users who use their platforms and services, to discern the boundary between lawful and unlawful online conduct and to organize their behavior accordingly. As a vast amount of human activity is now conducted online, such profound uncertainty about the law that governs it poses a grave threat to the public welfare. This Court's review of the proper scope and application of Section 230 is vital to ensure that the rule of law is upheld online.

II. The Wisconsin Supreme Court's maximalist view of Section 230 not only runs counter to the text and purpose of Section 230, but also distorts First Amendment doctrine and hinders the operation of the free market.

A. The history, text, and stated goals of Section 230 make clear that the statute was primarily intended to foster "Good Samaritan" behavior, that is, to remove disincentives for intermediaries to engage in self-regulation.

The heading of the operative subsection of Section 230 describes it as "Protection for 'Good Samaritan' blocking and screening of offensive material." This heading supplies important guidance as to the provision's intended meaning. *See Almendarez–Torres v. United States*, 523 U.S. 224, 234 (1998). In particular, it provides "a short-hand reference to the general subject matter" to which Congress meant to apply the provision. *Trainmen v. Balt. & Ohio R.R. Co.*, 331 U.S. 519, 528 (1947); *see also* Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 221 (2012) ("Titles and headings are permissible indicators of meaning.").

The concept of a Good Samaritan law is a familiar one in the United States. Such laws commonly provide immunity to people who attempt

to aid others in distress. *See*, *e.g.*, *Mueller v. McMillian Warner Ins. Co.*, 2006 WI 54, ¶ 30, 290 Wis. 2d 571, 714 N.W.2d 183. These laws, which exist in every state, provide an incentive for people to offer aid by removing the specter of liability for inadvertently harmful conduct. *See id. at* ¶¶ 39-46; *see also* Danny Veilleux, Annotation, *Construction and application of "good Samaritan" statutes*, 68 A.L.R.4th 294, § 2[a] (1989). In other words, Good Samaritan laws offer a limited form of protection in exchange for willingness to render aid.

The headings and structure of Section 230 make clear that its immunity provision was intended to be an online cognate of existing Good Samaritan laws. In addition to the explicit "Good Samaritan" reference in the heading, Section 230 immunizes providers and users of an interactive computer service from civil liability with regard to any action that is "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" or "taken to enable or make available to information content providers or others the technical means to restrict access" to such material. 47 U.S.C. § 230(c)(2).

In the offline context, it is obvious that Good Samaritan laws provide no protection to those who render no assistance, as the predicate acts that would create their potential liability would not exist.

More to the point, it would defy logic for Good Samaritan laws to protect those who not only fail to help, but who also actively engage in harmful activity. Yet, as this case illustrates, some interactive computer services argue for that perverse result under Section 230 for online activity.

The most extreme version of this view maintains, in effect, that interactive computer services are immune from liability simply because they traffic in third-party content. According to this misguided view, Section 230's safe harbor extends protection far beyond what the provision's words, context, and purpose support. Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 Fordham L. Rev. 401, 403 (2017). Decisions adopting this view have led to "outlandishly broad interpretations that have served to immunize platforms dedicated to abuse and others that deliberately host users' illegal activities." *Id.*

This extremely broad view is "hard to square with a plain reading of the statute," which clearly indicates that the "operative reasons for immunity" are screening and limiting access to objectionable content. Olivier Sylvain, *Intermediary Design Duties*, 50 Conn. L. Rev. 203, 239 (2018). The plain language and history of Section 230 cannot, in other words, support the view that the law grants immunity to providers or users of interactive computer services who make no effort to address objectionable content,

to say nothing of granting such immunity to those who actively promote or encourage unlawful activity. "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 harmful content. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U.L. Rev. 61, 116 n.377 (2009). Such service providers are Bad Samaritans—not entitled to the narrow protections intended to incentivize the self-regulation of online intermediaries. "None of the CDA's congressional purposes apply where platforms benefit from material's destructive nature. Extending immunity to Bad Samaritans undermines § 230's mission by eliminating incentives for better behavior by those in the best position to minimize harm." Citron & Wittes, *supra*, at 416.

B. The maximalist view of Section 230 surreptitiously and unjustifiably characterizes all online activity as speech.

Section 230 "always attempted to further two objectives: protecting ISPs from liability and thus fostering free speech, and encouraging ISPs to monitor and suppress offensive speech." Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 Geo. Wash. L. Rev. 986, 1010 (2008). Section 230's legislative findings and statements of its principal legislative sponsors focus on the importance of online communication for the flourishing of free speech and

providing "educational and informational resources to our citizens." 47 U.S.C. § 230(a)(1). "The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." *Id.* § 230(a)(3).

The maximalist approach to Section 230, however, goes far beyond fostering the kind of discourse and dissemination of ideas that is the core of the First Amendment. Indeed, one prominent commentator on Section 230 has said that the law is "better than the First Amendment" because it provides substantive and procedural protections beyond what First Amendment doctrine requires. Eric Goldman, *Why Section 230 Is Better Than the First Amendment* 8 (Mar. 12, 2019 draft) ("Section 230 expands the First Amendment's substantive scope … [and] provides extra procedural benefits to defendants. While the First Amendment sometimes mandates procedural as well as substantive rules, Section 230 offers more procedural protections, and greater legal certainty, for defendants.").[14] Though the commentator presents this as an outcome to be praised, it is actually cause for alarm. Section 230 has already been appropriated by "giant companies engaged in enterprises that have little to do with free expression." Citron & Wittes, *supra*, at 412.

[14] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3351323.

Armslist's enterprise—connecting sellers of deadly weapons with prohibited buyers for a cut of the profits—does nothing to provide "educational and informational resources" or contribute to "the diversity of political discourse." 47 U.S.C. § 230(a)(1), (3).

By viewing essentially all online conduct as the equivalent of free speech, the maximalist approach to Section 230 not only misconstrues the statue, but also threatens to distort the First Amendment itself. "Like any other rule, the First Amendment does not regulate the full range of human behavior. Rather, the Free Speech Clause of the First Amendment has a scope of application, and it is that scope of application that we can designate as its 'coverage.'" Frederick Schauer, *The Politics and Incentives of First Amendment Coverage*, 56 Wm. & Mary L. Rev. 1613, 1617–18 (2015). The First Amendment protects speech, not conduct. While some actions are sufficiently expressive to be considered speech for First Amendment purposes (*see, e.g., Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503 (1969) (wearing of black armbands conveyed message regarding a matter of public concern), conduct is not automatically protected simply because it involves language in some way. *Giboney v. Empire Storage & Ice Co.,* 336 U.S. 490, 502 (1949). ("[I]t has never been deemed an abridgement of freedom of speech or press to make a course of conduct illegal merely because the conduct was in part initiated, evidenced, or carried out by

means of language, either spoken, written, or printed."). What is more, not all speech receives full protection under the First Amendment. *See United States v. Stevens*, 559 U.S. 460, 468-69 (2010) (noting existence of "well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem" (citing *Chaplinsky v. New Hampshire,* 315 U.S. 568 (1942)).

So when "courts routinely interpret Section 230 to immunize all claims based on third-party content," including "negligence; deceptive trade practices, unfair competition, and false advertising; the common law privacy torts; tortious interference with contract or business relations; intentional infliction of emotional distress; and dozens of other legal doctrines," (Goldman, *supra*, at 6), this threatens to create a *sub rosa* expansion of First Amendment coverage. As Justice Powell worried, "[w]hen the coverage of the First Amendment expands … there is an increased possibility that, out of necessity, some of the existing doctrinal tools developed for a smaller area of coverage will have to be modified, possibly with unfortunate consequences." Schauer, *supra*, at 1635 (citing *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 456 (1978)).

In keeping with its text, structure, and history, Section 230 should not be construed as extending to all conduct occurring online. The

statute provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" and that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with [§ 230]." 47 U.S.C. § 230(c)(1), (e)(3). Section 230 does not state, and its findings and history do not support, that all possible conduct by users of online services, including illegal activity, can be considered "information." There is no basis for asserting that this provision broadly immunizes a website operator from liability for state-law claims related to the design and operation of a website that contains user-submitted content. Yet that is precisely how the Wisconsin Supreme Court misinterpreted Section 230 in the instant case.

Statements by Section 230's sponsors illustrate the dangers created by an overly broad interpretation of Section 230. Christopher Cox, a member of both the Reagan and George W. Bush Administrations as well as a former Republican Congressman who co-sponsored Section 230, observes "how many Section 230 rulings have cited other rulings instead of the actual statute, stretching the law," and maintains that "websites that are 'involved in soliciting' unlawful materials or 'connected to unlawful activity should not be immune under Section 230.'" Alina Selyukh, *Section 230: A*

Key Legal Shield For Facebook, Google Is About To Change, NPR (Mar. 21, 2018).[15] Senator Ron Wyden, a Democratic Senator and the other co-sponsor of Section 230, has similarly emphasized that "[t]he real key to Section 230 … was making sure that companies in return for that protection—that they wouldn't be sued indiscriminately—were being responsible in terms of policing their platforms." *Id.* Explaining his goals for Section 230, Senator Wyden said, "I wanted to guarantee that bad actors would still be subject to federal law. Whether the criminals were operating on a street corner or online wasn't going to make a difference." Ron Wyden, *Floor Remarks: CDA 230 and SESTA*, Medium (Mar. 21, 2018).[16]

As the Ninth Circuit stated, Section 230 was "not meant to create a lawless no-man's-land on the Internet." *Fair Housing Council v. Roommates.com, LLC*, 521 F.3d 1157, 1164 (9th Cir. 2008). That court explained:

> The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by

---

[15] https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change.

[16] https://medium.com/@RonWyden/floor-remarks-cda-230-and-sesta-32355d669a6e.

> 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., n.15. In line with that view, many scholars who have closely scrutinized the text, structure, and purpose of Section 230 have concluded that it should not be read to provide the kind of blanket immunity for all possible online activity that Armslist argued for, and the Wisconsin Supreme Court applied, here.

C. The maximalist interpretation of Section 230 also interferes with the operation of the free market by granting online intermediaries benefits that are unavailable to offline intermediaries.

The maximalist interpretation of Section 230 allows online intermediaries to immunize a far greater range of conduct than would be possible for offline intermediaries. As just one example, it grants

online intermediaries an advantage over offline intermediaries with regard to the scienter that would otherwise lead to civil or criminal liability under state law. "Section 230(c)(1)'s immunity does not vary with the Internet service's scienter. If a plaintiff alleges that the defendant 'knew' about tortious or criminal content, the defendant can still qualify for Section 230's immunity." Goldman, *supra*, at 7. As an example, the owner of a brick-and-mortar bookseller is potentially liable for unlawful material in her store once she is made aware of it, whereas an online bookseller remains immune from liability in the same circumstances.

The maximalist view of Section 230 also provides procedural benefits to online intermediaries not available to their offline counterparts. "Section 230 offers more procedural protections, and greater legal certainty, for defendants," by making it much easier for online intermediaries to defeat litigation at the motion to dismiss stage. *Id.*

The substantive and procedural benefits dictated by a maximalist interpretation of Section 230 are an unearned, anticompetitive advantage given to online businesses over their offline counterparts. If Congress had meant to grant such a broad business advantage to online entities, the narrow language of Section 230 would have been a curious way of doing so. As this Court has recognized, "Congress does not, one might say, hide elephants in mouseholes." *Puerto Rico v. Franklin*

Cal. Tax-Free Tr., 136 S. Ct. 1938, 1947 (2016) (citations and quotation marks omitted).

III. It is not overly burdensome for online intermediaries to engage in responsible design of their platforms and services.

Online intermediaries often claim that they are merely conduits for third-party content, such that requiring them to address harmful and possibly unlawful uses of their platforms and services is overly burdensome. But these enterprises are sophisticated entities that avidly employ technologically-advanced tools to maximize user engagement and their own profits. "Many of the most successful internet companies … design their applications to collect, analyze, sort, reconfigure, and repurpose user data for their own commercial reasons, unrelated to the original interest in publishing material or connecting users. These developments belie any suggestion that online intermediaries are merely conduits of user information anymore." Sylvain, *supra*, at 218.

The "neutral conduit" conception is often promoted by intermediaries well aware that their platforms and services are being used for harmful purposes: "Today, to the extent a company purports to be agnostic about its users' content, it generally does so mindful that its design will invite a wide range of content, including illegal or otherwise antisocial material." *Id.* Senator Wyden echoes this concern: "Tech giants cry that no one could track the

millions of posts or videos or tweets that cross their services every hour. But that's not what anybody's asking them to do! Section 230 means they are not required to fact-check or scrub every video, post, or tweet. But there have been far too many alarming examples of algorithms driving vile, hateful, or conspiratorial content to the top of the sites millions of people click onto every day—companies seeming to aid in the spread of this content as a direct function of their business models." Wyden, *supra*.

CCRI can directly attest to the ability and willingness of good-faith intermediaries to adopt design solutions against harmful uses of their platforms and services. Since 2014, CCRI has worked with tech companies such as Facebook, Twitter, and Google on responses to nonconsensual pornography and other abuses. Mary Anne Franks, "*Revenge Porn" Reform: A View from the Front Lines*, 69 Fla. L. Rev. 1251, 1272 (2017). In that time, every major tech platform banned nonconsensual pornography from their services and implemented reporting and removal policies. *Id.* These companies have continued to collaborate with CCRI and other nonprofit organizations to develop innovative responses to online abuse, including implementing photo-hashing technology and adjusting search-engine algorithms. *Id.*

When CCRI sought input from tech-industry leaders in drafting a 2016 federal criminal bill to prohibit nonconsensual pornography, one question

concerned their potential liability under the law. As Section 230 defenses do not apply to violations of federal criminal law, the bill had the potential to create criminal liability for online intermediaries. H.R. 5896, 114th Cong. (2016). CCRI and the congressional sponsors of the legislation did not wish to create liability for intermediaries who engaged in good-faith attempts to regulate nonconsensual pornography, but did want to hold accountable revenge porn sites that deliberately trafficked in such material. To that end, while the proposed legislation would impose liability on an individual who is reckless with regard to disclosures of prohibited content, it would only impose liability on an online intermediary if it "intentionally promotes or solicits" such content. Franks, *supra*, at 1295-96. The bill thus reflected the judgment, endorsed by several representatives of the tech industry, that it was not only fair, but affirmatively positive, for the law to distinguish between "good" and "bad" Samaritans. Indeed, Facebook and Twitter publicly supported the bill. *See* Press Release, Congresswoman Jackie Speier, *Congresswoman Speier, Fellow Members of Congress Take on Nonconsensual Pornography, AKA Revenge Porn* (July 14, 2016).[17]

[17] https://speier.house.gov/media-center/press-releases/congresswoman-speier-fellow-members-congress-take-nonconsensual.

IV. An overly expansive, textually unsupported interpretation of Section 230 particularly endangers the welfare and civil liberties of vulnerable groups, including domestic violence victims.

The death of Yasmeen Daniel's mother and three of her coworkers is hardly the only tragedy reportedly facilitated by Armslist:

- In 2012, a Russian immigrant named Demetry Smirnov shot 36-year-old Jitka Vesel 11-12 times in a museum parking lot after she rejected his advances, using a 40-caliber handgun he had purchased illegally through Armslist. Lorraine Bailey, *Murder Victim's Family Sues Gun Website*, Courthouse News (Dec. 14, 2012).[18]
- In 2018, a former US Marine reservist named Isaiah Janes killed himself with an AK-47 he purchased illegally through Armslist. Scott Glover, et al., *Cop convicted of illegal gun dealing sold weapon used in murder*, CNN (May 2, 2018).[19] Janes was prohibited from

[18] https://www.courthousenews.com/murder-victims-family-sues-gun-website/.

[19] https://www.cnn.com/2018/05/02/us/dc-cop-unlicensed-gun-dealer/index.html.

purchasing a weapon due to mental instability. He had previously attempted to buy a shotgun from a Dick's Sporting Goods store, but the sale was denied after the clerk conducted a required background check.

- Christopher Henderson used Armslist to traffic firearms to alleged gang members in Chicago, one of whom killed a 15-year-old boy named Xavier Soto in 2017. Madeline Buckley, *Gun trafficker tied to fatal shooting of 15-year-old boy given 5 1/2 years in prison*, Chicago Trib. (July 16, 2019).[20]
- A man named Muhammad Youssef Abdulazeez, who had recently been fired from his job at a nuclear plant, used Armslist to buy the weapons he used to kill five U.S. servicemen during a shooting spree in Chattanooga, Tennessee in 2015. Patrick Cooley, *Richfield man accused of selling guns to buyers in Beirut using controversial*

[20] https://www.chicagotribune.com/news/criminal-justice/ct-chicago-violence-gun-sentence-20190716-v6x2g2wluffzjhq7fw27hjpntu-story.html.

website, Cleveland.com (Nov. 20, 2015).[21]

- In 2018, Boston police officer Kurt Stokinger was shot in the leg by a convicted felon who had illegally purchased a firearm on Armslist. Steven Musil, *Boston cop sues online marketplace that sold gun used on him*, CNet (Oct. 18, 2018).[22]

And the list goes on.

The Wisconsin Supreme Court's extreme interpretation of Section 230 not only jeopardizes the safety and wellbeing of the general public, but particularly endangers the welfare and civil liberties of vulnerable groups. The instant case involves dangerous weapons being placed in the hands of violent domestic abusers—an outcome that diminishes the safety of every citizen, but particularly terrorizes and targets domestic violence victims, who are disproportionately female. Violence against women, from shootings to stalking to sexual assault, inflicts irreparable damage on society in the form of lost lives, physical injuries, financial costs, and gender inequality. The responsibility for that

---

[21] https://www.cleveland.com/metro/2015/11/richfield_man_accused_of_selli.html.

[22] https://www.cnet.com/news/boston-cop-sues-online-marketplace-that-sold-gun-used-on-him/.

damage lies not only with the individual perpetrators, but also with their tacit accomplices, including the online intermediaries whose greed renders them indifferent to dead bodies and silenced voices.

The Internet allows these accomplices to aggregate harm while disaggregating responsibility. It allows bad actors to hide behind keyboards as they contribute to campaigns of terror and violence against the most vulnerable groups in society, including women and minorities. *See* Danielle Keats Citron, *Hate Crimes in Cyberspace*, 13–15 (Harvard 2014); Eoin Blackwell, *The Internet Is Getting Nastier and Women and Minorities Are Feeling the Brunt of It*, Huffington Post (Oct. 23, 2017).[23] It enables individuals to set up virtual marketplaces in "third-party content" that includes everything from terrorism to election tampering while telling themselves—and courts—that they are merely providing "neutral platforms." If Section 230 is interpreted as Armslist urges—to immunize the knowing facilitation of dangerous and illegal transactions for profit, so long as that facilitation occurs online—this will provide succor not only to every reckless online arms broker, but also to every

[23] https://www.huffingtonpost.com.au/2017/10/22/ the-internet-is-getting-nastier-and-women-and-minorities-are-feeling-the-brunt-of-it_a_23249567/.

stalker, revenge pornographer, cop killer, and radical extremist.

The interpretation of Section 230 adopted by the Wisconsin Supreme Court will discourage efforts to restrict unlawful and harmful content—contravening the statute's purpose. Such a reading removes incentives for online intermediaries to redress harmful practices, no matter how easily they could do so. This radical, super-immunity creates a moral hazard, incentivizing intermediaries to act recklessly in pursuit of profit without fear of liability. *See* Mary Anne Franks, *Moral Hazard on Stilts: 'Zeran's' Legacy*, The Recorder (Nov. 10, 2017).[24]

It would allow intermediaries to generate revenue and free speech protections through every click or engagement, leaving users to bear the negative consequences. "Blanket immunity gives platforms a license to solicit illegal activity, including sex trafficking, child sexual exploitation, and nonconsensual pornography. Site operators have no reason to remove material that is clearly defamatory or invasive of privacy. They have no incentive to respond to clear instances of criminality or tortious behavior." Citron & Wittes, *supra*, at 414.

---

[24] https://www.law.com/therecorder/sites/therecorder/2017/11/10/moral-hazard-on-stilts-zeranslegacy/?slreturn=20190728195423

Over a decade ago, Professor Rebecca Tushnet warned that absolute immunity for online intermediaries, "even those that refuse to remove content after the original speaker concedes liability, or even those that deliberately induce the creation of content" for their own profit, creates "power without responsibility." Tushnet, *supra*, at 1010. As Yasmeen Daniel can attest, this power has already exacted too great a price.

CONCLUSION

Amici respectfully request that this Court grant the petition for certiorari.

Respectfully submitted,

Jeffrey A. Mandell
Counsel of Record
STAFFORD ROSENBAUM LLP
222 W. Washington Ave., #900
P.O. Box 1784
Madison, WI 53701-1784
jmandell@staffordlaw.com
608.256.0226

Counsel for Amici Curiae *The Cyber Civil Rights Initiative, Ann Bartow, Danielle Keats Citron, Dr. Mary Anne Franks, Woodrow Hartzog, Frank Pasquale, Neil Richards, Dr. Olivier Sylvain, and Dr. Ari Ezra Waldman*

August 30, 2019.