STATE OF WISCONSIN
SUPREME COURT

YASMEEN DANIEL, Individually, and as Special Administrator of the Estate of Zina Daniel Haughton,

Plaintiff-Appellant,

TRAVELERS INDEMNITY COMPANY OF CONNECTICUT, as Subrogee for Jalisco's LLC,

Intervening Plaintiff,

v.

ARMSLIST, LLC, an Oklahoma Limited Liability Company, BRIAN MANCINI, and JONATHAN GIBBON,

Defendants-Respondents-Petitioners,

BROC ELMORE, ABC INSURANCE CO., the fictitious name for an unknown insurance company, DEF INSURANCE CO., the fictitious name for an unknown insurance company, and ESTATE OF RADCLIFFE HAUGHTON, by his Special Administrator, Jennifer Valenti,

Defendants,

PROGRESSIVE UNIVERSAL INSURANCE COMPANY,

Intervening Defendant.

Appeal No. 2017-AP-344 Cir. Ct. No. 2015-CV-8710

BRIEF OF THE CYBER CIVIL RIGHTS INITIATIVE AND LEGAL SCHOLARS AS *AMICI CURIAE*

(Counsel for *Amici Curiae* listed on inside cover)

Jeffrey A. Mandell
State Bar No. 1100406
Gregory M. Jacobs
State Bar No. 1101064
STAFFORD ROSENBAUM LLP
222 West Washington Avenue, Suite 900
P.O. Box 1784
Madison, WI 53701-1784
jmandell@staffordlaw.com
gjacobs@staffordlaw.com
608.256.0226

Counsel for Amici Curiae
The Cyber Civil Rights Initiative,
Ann Bartow, Danielle Keats Citron,
Dr. Mary Anne Franks, Frank Pasquale,
and Olivier Sylvain

TABLE OF CONTENTS

TABLE OF AUTHORITIES

INTRODUCTION AND STATEMENT OF INTEREST

The Cyber Civil Rights Initiative ("CCRI") and undersigned law professors submit this brief as *amici curiae* in support of Plaintiff-Appellant Yasmeen Daniel with three purposes: first, to provide this Court with guidance as to the proper scope of immunity provided by Section 230 of the Communications Decency Act of 1996; second, to offer insight into the present ability of intermediaries to engage in responsible design of their platforms and services; and, third, to provide this Court with an account of how an overly expansive interpretation of Section 230 endangers the welfare and civil liberties of vulnerable groups in particular.

Amicus CCRI is a nonprofit organization dedicated to the protection of civil rights in the digital era. It is particularly concerned with abuses of technology that disproportionately impact certain groups, such as women and minorities. CCRI works with tech industry leaders, policymakers, courts, and law enforcement to address online abuses including "revenge porn" (the unauthorized disclosure of private, sexually explicit imagery), "doxing" (the release of private information for the purpose of harassment), and defamation. The organization provides support to victims of online abuse through its crisis

helpline, network of pro bono legal services, and guidelines for navigating reporting and removal procedures of online platforms. It also works with social media and technology 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. Two are members of CCRI's board: 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; and Secretary Danielle Keats Citron, a privacy expert and professor of law at Boston University School of Law (as of July 1, 2019) and professor of law at University of Maryland School of Law. They are joined in this brief by Ann Bartow, professor of law at the University of New Hampshire School of Law, Frank Pasquale, professor of Law at the University of Maryland School of Law, and Olivier Sylvain, professor of law at Fordham Law School.

ARGUMENT

I. Section 230 does not grant blanket immunity for unlawful or tortious activity simply because it takes place online instead of in physical space.

Section 230 provides in relevant part 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). Armslist and its supporting amici contend 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.

But as the Ninth Circuit observed, Section 230 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). As that court spelled out,

> 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., 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 that Armslist argues for here.

The text of Section 230 itself makes clear that providers are not broadly immunized for anything done in connection with the operation of a website. As the court below correctly observed, Section 230's grant of immunity is limited to those claims that treat the provider as a "publisher or speaker of any information provided by another." *Daniel v. Armslist, LLC*, 2018 WI App 32, ¶42, 382 Wis. 2d 241, 913 N.W.2d 211 (quoting 47 U.S.C. § 230).

Section 230's structure confirms the limits of this grant of immunity. The heading of the operative subsection 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. *Bhd. of R.R. Trainmen v. Baltimore & Ohio R.R. Co.*, 331 U.S. 519, 528 (1947).

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. Unfortunately, some courts—in decisions that are not binding on this Court—have endorsed this misguided view, extending Section 230's safe harbor far beyond what the provision's

words, context, and purpose support.[1] These decisions have led to "outlandishly broad interpretations that have served to immunize platforms dedicated to abuse and others that deliberately host users' illegal activities."[2]

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.[3] 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."[4]

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

---

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

[2] *Id.*

[3] Olivier Sylvain, *Intermediary Design Duties*, 50 Conn. L. Rev. 203, 239 (2018).

[4] Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 Geo. Wash. L. Rev. 986, 1010 (2008).

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.[5] 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."[6]

This conclusion is underscored further by both Section 230's legislative findings and statements of its principal legislative sponsors. The statute's own "findings" focus on the importance of ensuring the Internet's continued role in providing "educational and informational resources to our citizens." 47 U.S.C. § 230(a)(1). The text emphasizes the importance of online communication for the flourishing of free speech: "The Internet and other interactive computer services

---

[5] Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. Rev. 61, 116 n.377 (2009).

[6] Citron & Wittes, 86 Fordham L. Rev. at 416.

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). But Section 230 has been appropriated by "giant companies engaged in enterprises that have little to do with free expression."[7] 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."

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.'"[8] Senator Ron Wyden, a

---

[7] *Id.* at 412.

[8] Alina Selyukh, *Section 230: A Key Legal Shield For Facebook, Google Is About To Change*, NPR (Mar. 21, 2018), available at

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."[9] 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."[10]

The Court of Appeals correctly rejected a broad, atextual reading of Section 230 in favor of one that conforms closely to the statute's text, structure, and purpose.

II. Online intermediaries have the present ability 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 are increasingly

---

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

[9] *Id.*

[10] Ron Wyden, *Floor Remarks: CDA 230 and SESTA*, Medium (Mar. 21, 2018), available at https://medium.com/@RonWyden/floor-remarks-cda-230-and-sesta-32355d669a6e.

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."[11]

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."[12] 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

[11] Sylvain, 50 Conn. L. Rev. at 218.

[12] *Id.*

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."[13]

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.[14] In that time, every major tech platform banned nonconsensual pornography from their services and implemented reporting and removal policies.[15] 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.[16]

---

[13] Wyden, *supra* n.10.

[14] Mary Anne Franks, *"Revenge Porn" Reform: A View from the Front Lines*, 69 Fla. L. Rev. 1251, 1272 (2017).

[15] *Id.*

[16] *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.[17] CCRI and the legislation's congressional sponsors 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, the proposed legislation would impose liability on an individual who is reckless with regard to disclosures of prohibited content, but on an online intermediary only if it "intentionally promotes or solicits" such content.[18] The bill thus reflected the judgment, endorsed by several representatives of the tech industry, that it was not only fair, but affirmatively positive, to distinguish between "good" and "bad" Samaritans.[19]

---

[17] H.R. 5896, 114th Cong. (2016).

[18] Franks, 69 Fla. L. Rev. at 1295-96.

[19] 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*

III. An overly expansive, textually unsupported interpretation of Section 230 endangers the welfare and civil liberties of vulnerable groups in particular.

Armslist asks this Court to bless an interpretation of Section 230 that 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 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 aggregates these accomplices while disaggregating their responsibility. It allows bad actors to hide

---

Revenge Porn (July 14, 2016), available at https://speier.house.gov/media-center/press-releases/congresswoman-speier-fellow-members-congress-take-nonconsensual.

behind keyboards as they contribute to campaigns of terror and violence against the most vulnerable groups in society, including women and minorities.[20] It enables individuals to set up virtual marketplaces in "third-party content" that includes everything from terrorism to election tampering and tell themselves—and courts—that they are merely providing "neutral platforms." If Section 230 is interpreted as Armslist urges—to allow the knowing facilitation of dangerous and illegal transactions for profit with no consequences, so long as that facilitation occurs online—the result will provide succor not only to every reckless online arms broker, but also to every election hacker, revenge pornographer, and radical extremist.

If this Court interprets Section 230 in this way, its decision will discourage efforts to restrict unlawful and harmful content—contravening the statute's purpose. Such a reading would remove incentives for online intermediaries to redress harmful practices, no matter how easily they could do so. This radical, super-immunity would incentivize

---

[20] *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) available at 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/.

intermediaries to act recklessly in pursuit of profit without fear of liability. 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."[21]

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."[22] As Yasmeen Daniel can attest, this power has already exacted too great a price.

---

[21] Citron & Wittes, 86 Fordham L. Rev. at 414.

[22] Tushnet, 76 Geo. Wash. L. Rev. at 1010.

CONCLUSION

For the foregoing reasons, the Court of Appeals judgment should be affirmed.

Dated: January 24, 2019

STAFFORD ROSENBAUM LLP

By _____
Jeffrey A. Mandell
State Bar No. 1100406
Gregory M. Jacobs
State Bar No. 1101064

Counsel for Amici Curiae
The Cyber Civil Rights Initiative, Ann Bartow, Danielle Keats Citron, Dr. Mary Anne Franks, Frank Pasquale and Olivier Sylvain

222 West Washington Avenue,
Suite 900
P.O. Box 1784
Madison, Wisconsin 53701-1784
jmandell@staffordlaw.com
gjacobs@staffordlaw.com
Telephone: (608) 256-0226
Facsimile: (608) 259-2600

FORM AND LENGTH CERTIFICATION

I hereby certify that this brief conforms to the rules contained in section 809.19(8)(b) and (c) for a brief produced with a proportional serif font.

The length of this brief is 3,000 words.

Dated: January 24, 2019.

Jeffrey A. Mandell

CERTIFICATION REGARDING ELECTRONIC BRIEF

I hereby certify that I have submitted an electronic copy of this brief, which complies with the requirements of Wis. Stat. § 809.19(12).

I further certify that the text of the electronic copy of the brief is identical in content and format to the printed form of the brief filed as of this date.

A copy of this certificate has been served with the paper copies of this brief filed with the court and served on all opposing parties.

Dated: January 24, 2019.

Jeffrey A. Mandell

CERTIFICATION OF FILING AND SERVICE

I certify that the brief was hand delivered to the Clerk of the Supreme Court on January 24, 2019.

I further certify that, on January 24, 2019, three copies of the brief were mailed via U.S. Mail to:

Patrick O. Dunphy
Brett A. Eckstein
P.O. Box 1750
Brookfield, WI 53008-1750

Jacqueline C. Wolff
Samantha J. Katze
7 Times Square
New York, NY 10036

Jonathan E. Lowy
Suite 400
840 First St NE
Washington, DC 20002

Joshua D. Maggard
Eric J. Van Schyndle
James E. Goldschmidt
411 E. Wisconsin Ave., Ste. 2400
Milwaukee, WI 53202

John F. Fuchs
Suite 100
13500 Watertown Plank Road
Elm Grove, WI 53122

John A. Griner, IV
13935 Bishops Dr., Ste. 250
Brookfield, WI 53005-6605

Thomas M. Devine
Anthony Hahn
840 Lake Ave., Ste. 300
Racine, WI 53403-1566

Crystal N. Abbey
P.O. Box 785
Appleton, WI 54912-0785

Brian T. Fahl
825 N. Jefferson St. 5th Floor
Milwaukee, WI 53202-3737

Anthony J. Dreyer
Elizabeth A. Hellman
Naomi S. Solomon
4 Times Square
New York, NY 10036

Michael J. Dell
Karen S. Kennedy
1177 Avenue of the Americas
New York, NY 10036

Kathryn A. Keppel
Steven C. McGaver
330 E. Kilbourn Ave., Ste. 1170
Milwaukee, WI 53202

Andrew Thomas Dufresne
1 E. Main St., Ste. 201
Madison, WI 53703-5118

John C. Peterson
Emily I. Lonergan
P.O. Box 2700
Appleton, WI 54912-2700

Guy DuBeau
P.O. Box 1767
Madison, WI 53701-1767

Erin G. Sutton
Leonard A. Nelson
330 N. Wabash Ave., Ste. 39300
Chicago, IL 60611

Peyton B. Engel
Marcus J. Berghahn
P.O. Box 1528
Madison, WI 53701-1528

I further certify that the brief was correctly addressed and postage was prepaid.

Dated: January 24, 2019.

Jeffrey A. Mandell