University of Miami Business Law Review

Volume 29 | Issue 2 Article 5

Analysis Of Section 230 Under a Theory of Premises Liability: A Focus on *Herrick v.Grindr* and *Daniel v. Armslist*

Kassandra C. Cabrera
University of Miami School of Law

Follow this and additional works at: https://repository.law.miami.edu/umblr

 Part of the Business Organizations Law Commons, and the Internet Law Commons

Recommended Citation

Kassandra C. Cabrera, *Analysis Of Section 230 Under a Theory of Premises Liability: A Focus on Herrick v.Grindr and Daniel v. Armslist*, 29 U. MIA Bus. L. Rev. 53 ()
Available at: https://repository.law.miami.edu/umblr/vol29/iss2/5

This Comment is brought to you for free and open access by the Journals at University of Miami School of Law Institutional Repository. It has been accepted for inclusion in University of Miami Business Law Review by an authorized editor of University of Miami School of Law Institutional Repository. For more information, please contact library@law.miami.edu.

Analysis Of Section 230 Under a Theory of Premises Liability: A Focus on *Herrick v. Grindr* and *Daniel v. Armslist*

Kassandra C. Cabrera

Abstract

Section 230 of the Communications Decency Act ("CDA") has been held to give online service providers acting as interactive computer services sweeping immunity for content posted on their platforms. The intention behind the creation of Section 230 was not to immunize online service providers from all liability. Rather, Section 230 was enacted to protect online intermediaries acting as "Good Samaritans"—those who made "good faith" efforts to restrict unlawful or harmful content, but due to the breadth of the internet and advancements in technology over or under-filtered content on their platforms. This note outlines an approach for courts to hold online service providers liable for the foreseeable consequences of harmful content on their platforms. Under a theory of premises liability, online service providers can be held liable for the foreseeable consequences of dangerous, harmful, or illegal content made by third parties and allowed on their platforms. In other words, like physical landowners or business operators, online service providers should have a duty to maintain their websites in a reasonably safe condition and to protect against, and remedy, harmful third-party content by making "good faith" efforts to moderate content. Generally, the owners of physical locations open to the public have a duty to make reasonable efforts to protect people against foreseeable harm caused by the acts of third parties that they know, or should know about, and that are likely to occur without such efforts. That same duty should be extended to the online context. By extending a duty similar to that required in the theory of premises liability, online platforms will be incentivized to implement measures to prevent future damage and rectify any potentially dangerous conditions

present once having been informed of such. Only when online intermediaries make reasonable, "good faith" moderation efforts, should they be given immunity under Section 230. Thus, applying the theory of premises liability to the online context would serve the purpose of Section 230 better than the status quo. Specifically, this note applies the theory of online premises liability by applying it to two cases that were submitted to the United States Supreme Court for review this term—Herrick v. Grindr (review denied on October 7, 2019) and Daniel v. Armslist (review denied on November 25, 2019). This analysis will demonstrate how the imposition of a duty similar to that of premises liability will incentivize online operators to implement measures to prevent against foreseeable harm.

I. INTRODUCTION

In the last twenty years, the Internet has grown to become home to over 1.75 billion websites.[1] Internet activity is dominated by multi-billion-dollar companies that profit from content posted by third parties—these include, but are not limited to, Facebook, Twitter, YouTube, and Craigslist. In 1996, prior to the immense and unimaginable expansion of the Internet, Congress passed Section 230 of the Communications Decency Act ("CDA").[2] Representatives Christopher Cox and Ron

---

1 *Total Number of Websites,* internet live stats (retrieved on February 21, 2020), https://www.internetlivestats.com/total-number-of-websites/.

2 47 U.S.C. § 230 ("Communications Decency Act" or "CDA").

Wyden, the drafters of Section 230, propelled it through Congress with the intent of establishing the foundation for a safe and free Internet.[3]

Section 230(c) is titled "Protection for "Good Samaritan" Blocking and Screening of Offensive Material".[4] Section 230(c)(1) of the CDA states,

> "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."[5]

According to Section 230(c)(2),

> "No provider or user of an interactive computer service shall be held liable on account of—any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected . . . ."[6]

Section 230 distinguishes interactive computer services from online content providers.[7] An online content provider is one who creates content—for example, by making a statement[8]—while an interactive computer service provides the means to do so. Many interactive service providers not only provide a platform for content but also promote, sort, and shape third-party posts. An interactive computer service, like Facebook or YouTube, acts as a host for content, while online content providers develop or contribute content.[9] In the Electronic Frontier Foundation's description, Section 230 establishes that "online intermediaries that host or republish speech are protected against a range

---

3 *See* Felix Gillette, *Section 230 Was Supposed to Make the Internet a Better Place. It Failed,* BLOOMBERG BUSINESSWEEK (Aug. 7, 2019), https://www.bloomberg.com/news/features/2019-08-07/section-230-was-supposed-to-make-the-internet-a-better-place-it-failed.

4 47 U.S.C. § 230(c).

5 47 U.S.C. § 230(c)(1).

6 47 U.S.C. § 230(c)(2)(A).

7 *See* 47 U.S.C. § 230 (f)(2)-(3).

8 *See* 47 U.S.C. § 230(f)(3).

9 *See* Jeff Kosseff, *What's in a Name? Quite a Bit, If You're Talking About Section 230*, LAWFARE (Dec. 19, 2019), https://www.lawfareblog.com/whats-name-quite-bit-if-youre-talking-about-section-230 ("[Section 230] provides online platforms such as websites and social media services with broad protection from liability arising from many types of user-generated content.").

of laws that might otherwise be used to hold them legally responsible for what others say and do."[10]

The idea behind Section 230 was to provide online service providers with immunity when they acted as "Good Samaritans" in addressing harmful content posted by third parties on their platforms.[11] After diligently researching the history of Section 230 for over two years for his book *The Twenty-Six Words That Created the Internet,* Jeff Kosseff found that "Congress passed Section 230 to empower consumers and platforms—rather than the government—to develop the rules of the road for the nascent commercial internet."[12] Section 230 was intended to serve dual purposes: (c)(1) was designed to remove the burden of treating online intermediaries as publishers and (c)(2) was intended to incentivize "good faith" content moderation practices.[13] Despite this, most online platforms have failed to adequately moderate, or moderate content at all. As a result, multi-billion-dollar internet companies have been granted immunity for allowing, or even promoting, content that severely negatively affects their users, and others, often by ignoring easily implementable protective and remedial moderation measures.[14]

By contrast, brick and mortar businesses have been held to share liability for the harmful conduct caused by third parties in their physical operating locations. The concept of collective responsibility considers those exercising control over a particular space, like a business operator or landowner, responsible for "harmful acts they did not cause but did not do enough to prevent."[15] For example, a hotel can be sued for a shooting by a

---

[10] *Section 230 of the Communications Decency Act,* ELECTRONIC FRONTIER FOUNDATION (last visited on Feb. 2, 2020), https://www.eff.org/issues/cda230.

[11] *See* 47 U.S.C. § 230(c)(1)-(2).

[12] Kosseff, *supra* note 9.

[13] *See* § 230(c)(1); *see* § 230(c)(2); *Section 230 Workshop—Nurturing Innovation or Fostering Unaccountability?*, THE U.S. DEP'T. OF JUST. (Feb. 19, 2020), https://www.justice.gov/opa/video/section-230-workshop-nurturing-innovation-or-fostering-unaccountability (referring to Mary Anne Franks at 2:16:40) (stating that (c)(2) protects "Good Samaritans" but what it offers is taken away by (c)(1) which has been held to mean that platforms will not be held accountable even if they don't).

[14] *See* Danielle Keats Citron & Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, 2 GEO. L. TECH. L. REV. 453, 466 (2018) (providing a list of entities that are "immunized from liability" under a general reading of Section 230).

[15] Mary Anne Franks, *Our Collective Responsibility for Mass Shootings*, THE NEW YORK TIMES (Oct. 9, 2019) https://www.nytimes.com/2019/10/09/opinion/mass-shooting-responsibility.html ("The MGM settlement illustrates the principle of collective responsibility, under which third parties can be considered responsible for harmful acts they did not cause but did not do enough to prevent . . . .Such entities are often said to have breached a 'duty of care,' and imposing liability is intended to give them incentive to be more careful in the future.").

third-party that occurred on its premises;[16] a motel can be sued for the rape and murder of a woman committed by a third-party;[17] and a store can be sued for failing to rectify a dangerous condition caused by a third party.[18] These brick and mortar businesses have been held collectively responsible for failing to protect against dangerous conditions that were reasonably likely to result in harm or for failing to respond adequately to remedy potentially dangerous conditions they knew or should have known would result in harm.[19] Online service providers, by contrast, have not been found to be collectively responsible for harmful content allowed or facilitated by their platforms.

Online service providers—against which many brick and mortar businesses continue to compete—have swaddled themselves and their wrongdoing in the blanket immunity granted to them by courts around the country through Section 230. Despite the differences between virtual and physical spaces, a duty analogous to that in premises liability—which would require interactive computer services to maintain their online operations in a reasonably safe condition by practicing "good faith" efforts—should be extended to the online context.[20] While premises liability cannot be extended literally to the online context, many of its principles—like that of foreseeability of harm, specifically—can be meaningfully applied. "The important similarity is that offline and online business owners establish, control, and benefit from their businesses. Website operators are proprietors who exercise control over their business in many ways."[21] Website operators are in the best position to protect their users and have the resources to do so.

---

16 *See* Marco della Cava, *'This is mercy, not justice': Las Vegas Shooting Victims to Split $800M. But How Much is Pain Worth?*, USA TODAY (Dec. 6, 2019), https://www.usatoday.com/story/news/nation/2019/12/06/las-vegas-shooting-victims-split-mgm-settlement-judges-decide/2601704001/.

17 David J. Neal and Johanna Alvarez, *She Spent Her Last Night at a Motel. The Motel Owes her Mother and Father $12 Million.*, MIAMI HERALD (Dec. 4, 2017), https://www.miamiherald.com/news/local/community/miami-dade/hialeah/article188070239.html.

18 Joe Marusak, *Woman Sues Walmart After Slipping on Blueberries, Causing 'Unbearable Pain'*, THE CHARLOTTE OBSERVER (May 30, 2019), https://www.charlotteobserver.com/news/local/article230957738.html.

19 Ann M. v. Pac. Plaza Shopping Ctr., 6 Cal. 4th 666, 674 (1993) (stating that premises liability is a subcategory of negligence torts, where a plaintiff claims that the defendant failed to 'maintain land in their possession and control in a reasonably safe condition.').

20 *See* Nancy S. Kim, *Website Proprietorship and Online Harassment*, 2009 UTAH L. REV. 993, 1034 (2009) ("[T]he analogy to premises liability is not a perfect one given the differences between the Internet and the physical world, including the inability to draw secure boundaries and screen for potential harm.").

21 *Id.*

Although Section 230 was designed with a focus on preserving the First Amendment,[22] much of what Section 230 has been found to protect transcends speech and crosses into the realm of conduct.[23] This is a point emphasized by Carrie Goldberg, the attorney for the Plaintiff in *Herrick v. Grindr.* At a Department of Justice Workshop regarding Section 230 on February 19, 2020, Goldberg spoke of how much of the litigation surrounding Section 230—including that which occurred in the case of her client—is not about words, but actions.[24]

> It's centuries of tort law that empowers an individual to get justice when they are being harmed . . . And when a platform . . . basically hides behind Section 230 as the standard of care that allows them to do nothing, then that's an access to justice issue. This isn't about speech, because a lot of these lawsuits have to do with conduct, not content. Let Section 230 exist and regulate content. People should be able to call one another the b-word on twitter without being sued . . . but it's gone too far.[25]

A longstanding exception to First Amendment protection is speech that is "integral to criminal [or tortious] conduct.[26] For example, the Supreme Court has extended this exception to prohibit "distributing and possessing child pornography, [ ] soliciting crime, and [ ] announcing discriminatory policies."[27] Furthermore, in *United States v. Osinger*, the Ninth Circuit Court of Appeals upheld the Federal Cyberstalking statute because it prohibited harassing and intimidating conduct, not speech protected by the First Amendment.[28] Thus, the fact that an act involves speech does not mean that it cannot also constitute conduct.[29] The

---

[22] Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*, UNIV. CHICAGO LEGAL FORUM 6 (forthcoming 2020).

[23] *Id.* ("Immunizing from liability enterprises that have nothing to do with moderating online speech, such as marketplaces that connect sellers of deadly weapons with prohibited buyers for a cut of the profit, is unjustifiable.").

[24] THE UNITED STATED DEP'T. OF JUSTICE, *supra* note 13 (referring to Carrie Goldberg).

[25] *Id.* (referring to Carrie Goldberg at 1:26:20).

[26] Eugene Volokh, *Speech Integral to Criminal Conduct*, 101 CORNELL L. REV. 981, 983 (2016) (citing United States v. Alvarez*,* 132 S. Ct. 2537, 2544 (2012) (plurality opinion); Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2665 (2011); Holder v. Humanitarian Law Project, 561 U.S. 1, 27 n.5 (2010); United States v. Stevens, 559 U.S. 460, 468–69 (2010); United States v. Williams, 553 U.S. 285, 297 (2008); Rumsfeld v. FAIR, 547 U.S. 47, 62 (2006)).

[27] Volokh, *supra* note 26; *see* New York v. Ferber, 458 U.S. 747, 761–62 (1982); *Williams*, 553 U.S. at 297; *Rumsfeld*, 547 U.S. at 62.

[28] *See* United States v. Osinger, 753 F.3d 939, 944 (9th Cir. 2014).

[29] *See* United States v. O'Brien, 391 U.S. 367, 376 (1968).

summaries of *Herrick v. Grindr* and *Daniel v. Armslist* provided in Part IV of this note further illustrate this point.

What is more, if the underlying purpose of Section 230 was to promote speech, failing to address online abuse significantly hinders that goal. Victims of online abuse have a higher tendency to suppress their speech than others.[30] Such self-censorship diminishes the marketplace of ideas, which undermines a fundamental goal of the First Amendment.[31]

Applying premises liability—which originated in common law and has been imposed on the owners of physical spaces for decades[32]—to online service providers essentially means holding them liable for the dangerous conduct allowed, or inadequately addressed, on their platforms.[33] This theory focuses on foreseeable consequences.[34] Typically, land operators, businesses or owners, are held responsible for failing to implement reasonable precautions for, or failing to reasonably respond to, dangerous third-party conduct or conditions that can foreseeably result in harm.[35] There are exceptions under this theory for holding landowners or operators liable for open and obvious dangerous conditions[36] and for harm which they lacked actual or constructive knowledge of.[37] Thus, to successfully sue under a theory of premises liability, a plaintiff must demonstrate that the defendant breached its duty by failing to take reasonable precautions against potentially dangerous or harmful conditions it knew or should have known about, and which was not openly obvious to the plaintiff so that he or she could avoid it.[38]

Online service providers should be extended a duty to take reasonable precautions to protect against foreseeable consequences of dangerous third-party content. Today, numerous courts across the country have extended immunity to online service providers who have done close to nothing, or nothing at all, to protect against ongoing or potential future harm, regardless of whether they are being treated as publishers. As a

---

30 Citron & Franks, *supra* note 22 at 9 (citing to Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use,* 31 BERKELEY TECH. L.J. 117, 125-26 (2016)).

31 *See id.* at 9-10.

32 *See* Robert S. Driscoll, *The Law of Premises Liability in America: Its Past, Present, and Some Considerations for its Future*, 82 Notre Dame L. Rev. 881, 881 (2013) (describing the change in standard from the landmark decision of *Rowland v. Christian,* 443 P.2d 561 (Cal. 1968)).

33 *See, e.g.,* Martin v. Rite Aid of Pennsylvania, Inc., 80 A.3d 813, 815 (Pa. Super. Ct. 2013) ("[P]ossessors of land who hold it open to the public . . . owe a duty to any business invitee . . . to take reasonable precaution against harmful third-party conduct that might be reasonably anticipated.").

34 RESTATEMENT (SECOND) OF TORTS § 343 (1965).

35 *See Rite Aid of Pennsylvania, Inc.*, 80 A.3d at 815 (2013).

36 *See* Richard v. Meijer, No.342766, 2019 *WL* 1780670 (Apr. 23, 2019).

37 *See* Waldon v. Wal-Mart Stores, Inc., 943 F.3d 818, 822 (7th Cir. 2019).

38 RESTATEMENT (SECOND) OF TORTS § 343 (1965).

result, online service providers are not incentivized to discover and implement reasonable precautions because they are guaranteed immunity regardless of what measures, or lack thereof, that they choose to implement, and whether or not they are being treated as publishers. Users, and others in the community, suffer the consequences of dangerous third-party conduct that is facilitated by these online platforms.[39] Therefore, Section 230's preemptive immunity should be granted only when the online service provider is actually being treated as a publisher, otherwise the online service provider should be extended a duty of care.

The concept of willful ignorance—which is used in determining criminal culpability—allows a defendant to be found guilty of a crime requiring knowledge because the defendant willfully ignored the facts.[40] Under the theory of premises liability, a defendant can be found to be liable for negligently maintaining his property when there is a reasonable likelihood of harm that is foreseeable, even if the defendant chooses to ignore the foreseeability of that harm. Additionally, the concept of willful ignorance is contrary to Section 230's "good faith" requirement.[41] Proof of foreseeability for negligence does not require a showing of actual knowledge, but only that the defendant knew or should have known.[42]

By extending a duty of care to online service providers, courts would incentivize the platforms to make risk assessments and engage in cost benefit analyses to determine which safety features to implement.[43] Thus, rather than granting *all* online service providers immunity, courts would only give immunity in cases where online service providers are treated as publishers, as per the language of Section 230. Further, Courts would only impose liability on those providers who have failed to make "good faith" efforts to moderate content to protect users from foreseeably dangerous third-party content.

---

39 Mary Anne Franks, *Moral Hazard on Stilts: 'Zeran's' Legacy*, THE RECORDER (Nov. 10, 2017), https://www.law.com/therecorder/sites/therecorder/2017/11/10/moral-hazard-on-stilts-zerans-legacy/ ("Today, the Internet is awash in threats, harassment, defamation, revenge porn, propaganda, misinformation, and conspiracy theories, which disproportionately burden vulnerable private citizens including women, racial and religious minorities, and the LGBT community. They are the ones who suffer while the websites, platforms, and ISPs that make it possible for these abuses to flourish are protected from harm.").

40 *See* Alexander F. Sarch, *Beyond Willful Ignorance*, 88 UNIV. COL. L. REV. 97, 101 (2017).

41 47 U.S.C. § 230(c).

42 RESTATEMENT (SECOND) OF TORTS § 343 (1965).

43 *See Prepared Written Testimony and Statement for the Record For Hearing on Fostering a Healthier Internet to Protect Consumers Before the H. Comm. on Energy and Commerce*, 116th Cong. (Oct. 16, 2019) (statement of Danielle Keats Citron, Professor of Law, Boston University School of Law) ("Congress wanted to incentivize private efforts to filter, block, or otherwise address troubling online activity.")

It is important to note that this does not mean that online service providers must protect against *all* dangerous third-party content and conduct. This simply means that online service providers will not be given the immunity shield unless they have used their sword by acting within their power to reasonably protect against and rectify dangerous conditions.[44] By analyzing cases of online harms through a premises liability lens, courts can better serve the purpose of Section 230 by incentivizing online service providers to make good faith efforts to protect Internet users against foreseeable harm.[45] Otherwise, these multi-million and billion-dollar online service providers will continue to operate unscathed despite their flagrant disregard for user safety, and public safety generally.

Part II explains the intent and purpose of Section 230 by looking at the statute's history and its evolution of its interpretation by courts. Part III describes the theory of premises liability, focusing on various approaches courts have taken in applying it and identifying the best approach for the online context. Part IV explains how the theory of premises liability could successfully be used by courts to apply Section 230 in a way that incentivizes online service providers to engage in "good faith" content moderation and adhere to principles applied to physical spaces, focusing on extending a duty to online service providers and examining causation requirements. Specifically, this note will apply premises liability concepts to the cases of *Herrick v. Grindr* and *Daniel v. Armslist* in a way that promotes Section 230's goal of incentivizing online service providers to act in "good faith" to reasonably protect users against foreseeable harm.

In *Grindr*, the Second Circuit Court of Appeals affirmed the Southern District of New York's determination that Grindr was immune from liability despite having substantial knowledge of dangerous conditions and failing to take reasonable measures, or any measures for that matter, to prevent negative consequences. Unlike in *Herrick*, the appellate court in *Daniel v. Armslist* declined to find that Section 230 immunized Armslist from liability. The court found that the plaintiff was not attempting to treat

---

[44] Felix Gillette, *Section 230 Was Supposed to Make the Internet a Better Place. It Failed*, BLOOMBERG BUSINESSWEEK (Aug. 7, 2019), https://www.bloomberg.com/news/features/2019-08-07/section-230-was-supposed-to-make-the-internet-a-better-place-it-failed (quoting Representative Wyden stating, "There was a shield, and there was a sword. The sword was the legal authority of the website owner to moderate content. It's clear to me looking at the evolution of time that too many sites—particularly the big companies as they got so prosperous—enjoyed the shield, but weren't willing to use the sword.").

[45] *See* Danielle Keats Citron, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, 86 FORDHAM L. REV. 401, 416 (2017) ("[The current] interpretation undermines the congressional goal of incentivizing self-regulation.").

Armslist as a publisher of third-party content, which would contravene Section 230 (c)(1), but instead sought to hold Armslist liable for its negligent conduct in the creation and operation of its own platform. As a result, Armslist was not able to dismiss the case on Section 230 grounds. However, the Wisconsin Supreme Court reversed this ruling and, like the New York court in *Grindr,* found that 230 immunity did in fact apply. The U.S. Supreme Court denied review in *Herrick v. Grindr* on October 7, 2019 and *Daniel v. Armslist*, on November 25, 2019, leaving the prior decisions in place.

The outcomes in these two cases are hard to imagine in the physical world.[46] "[I]n physical spaces, individuals or businesses that fail to 'take care' that their products, services or premises are not used to commit wrongdoing can be held accountable for that failure. It is no less important that this duty to take care be honored in virtual spaces."[47] However, courts have abandoned classical tort theories in deciding cases occurring in virtual spaces.[48] Courts should apply the tort theory of premises liability to the online context so that immunity for online service providers exists only for platforms that have taken reasonable measures to protect from dangerous conditions or prevent harm of which they know, or should know, is reasonably likely to occur.

Recently, Congress has debated the language and application of Section 230, and some members have even discussed repealing it.[49] Although Section 230 has in fact resulted in unacceptable consequences, we must not forget its positive effect on the creation of the expansive Internet we have today.[50] Jeff Kosseff stated, "[w]e don't need to choose between the status quo and an all-out repeal of Section 230, however. Instead, platforms should immediately revamp their content moderation policies and procedures, as some are now starting to do, beginning with more moderators and better automated technology."[51] However, it is up to the courts to hold these online service providers liable for failing to take reasonable measures in order to incentivize them to "revamp their content moderation policies and procedures"[52] as Kosseff suggests.

---

46 *See* Franks, *supra* note 15 (stating that MGM's attempt to avoid liability for failing to secure its premises was met with outrage by the general public).

47 *Id.*

48 *See* THE UNITED STATED DEP'T. OF JUSTICE, *supra* note 13 (referring to Carrie Goldberg at 1:26:20).

49 *See* Press Release, Dep't of Justice to Hold Workshop on Section 230 of the Commc'ns Decency Act (Jan. 30, 2020).

50 Jeff Kosseff, *Op-Ed: Section 230 created the Internet as we know it. Don't mess with it.*, LOS ANGELES TIMES (Mar. 29, 2019) https://www.latimes.com/opinion/op-ed/la-oe-kosseff-section-230-internet-20190329-story.html.

51 *Id.*

52 *Id.*

II. SECTION 230's HISTORY AND JUDICIAL INTERPRETATION

Section 230 regulates the liability of website operators such as social media platforms and online marketplaces for user-generated content. The history that led to the passage of Section 230 indicates that the provision was intended to encourage "good faith" content moderation by online service providers.[53] By extending practically absolute immunity to online service providers, courts have precluded incentivizing online service providers to adopt reasonable protective measures.[54] Furthermore, the outcomes in cases concerning liability, or lack thereof, of online service providers, would be considered unacceptable if their origin were in a physical rather than virtual space. Analyzing cases involving Section 230 under a theory of premises liability—a theory that has historically be applied in physical spaces—endorses the implementation of practices that will lead to a safer internet.

The story of Section 230 in many ways begins with the cases of *Cubby, Inc. v. Compuserve*, *Inc.* and *Stratton Oakmont, Inc. v. Prodigy Servs. Co.* In *Compuserve*, the defendant hosted an "online general information service or 'electronic library.'"[55] Subscribers had access to tons of information as well as access to online forums, one of which was the Journalism Forum.[56] Rumorville USA ("Rumorville") was a daily newsletter available as part of the Journalism Forum.[57] The plaintiffs alleged that Rumorville, a news and gossip database, "published false and defamatory statements relating to Skuttlebut", its competitor,[58] and argued that Compuserve was the carrier of these statements.[59] The District Court held that Compuserve could be held liable for Rumorville's posts if Cubby could demonstrate that it knew or should have known of the statements defamatory nature, and there was no evidence of such.[60] Compuserve chose not to review Rumorville's posts, and thus exercised no editorial control.[61] Thus, Compuserve was found to be immune from liability

---

53 *See* Citron & Wittes, *supra* note 14 at 461 ("Section 230 was by no means meant to immunize services whose business is the active subversion of online decency—businesses that are not merely failing to take steps to protect users from online indecency but are actually facilitating and encouraging online illegality.").

54 *Id.* at 465 ("The broad sweeping interpretation of Section 230's immunity eliminates incentives for better behavior by those in the best position to minimize harm.").

55 Cubby, Inc. v. Compuserve, Inc., 776 F.Supp. 135, 137 (S.D. N.Y. 1991).

56 *Id.*

57 *Id.*

58 *Id.* at 138.

59 *Id.*

60 *Id.* at 141.

61 *Id.*

because it did not know about the nature of the statements and had not exercised control over the content of Rumorville's posts.[62]

Contrarily, in *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, Prodigy operated an online message board that employed editors for the content posted on these message boards.[63] One message board post by a third-party allegedly defamed Stratton Oakmont, which then sued Prodigy for failing to fully moderate the content posted on its message board.[64] Despite having approximately 60,000 postings a day, a number difficult to moderate, the court found that because Prodigy moderated some of the content posted on its message board it could be held liable for harmful content it did not remove.[65] Essentially, the court's holding meant that "[t]o avoid liability, the company would have to give up moderating all together and simply act as a blind host . . . ."[66]

In response to the court's decision in *Prodigy,* Representatives Christopher Cox and Ron Wyden proposed an amendment to the CDA. It is important to note that in 1996, the year the amendment was passed, the Internet was not, nor was it likely ever imagined to become, what it has grown into today.[67] Representative Cox has stated that "[t]he original purpose of [Section 230] was to help clean up the Internet, not to facilitate people doing bad things on the Internet."[68] The policy, as stated by the statute itself, echoes Representative Cox's underlying reasoning for Section 230. As per Section 230, the statute was designed in part to promote free market ideals and development of the Internet while enforcing federal criminal laws by deterring and punishing unlawful activity in the online context.[69] "The Cox-Wyden Amendment, codified in

---

62 *Id.*

63 Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (Sup. Ct. Nassau County 1995).

64 *Id.*

65 *CDA 230: Legislative History*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/cda230/legislative-history (last visited on Nov. 1, 2019) (referring to *Stratton Oakmont v. Prodigy Servs. Co.,* 1995 WL 323710 (Sup. Ct. Nassau County 1995).

66 *Id.*

67 Danielle Keats Citron, *Section 230's Challenge to Civil Rights and Civil Liberties*, KNIGHT FIRST AMENDMENT INSTITUTE (Apr. 6, 2018), https://knightcolumbia.org/content/section-230s-challenge-civil-rights-and-civil-liberties.

68 Alina Selyukh, *Section 230: A Key Legal Shield for Facebook, Google Is About to Change*, NPR, https://www.npr.org/sections/alltechconsidered/2018/03/21/591622450/section-230-a-key-legal-shield-for-facebook-google-is-about-to-change (Mar. 21, 2018 5:11 am EDT).

69 47 U.S.C. § 230(b); *see* Mary Anne Franks, *The Lawless Internet? Myths and Misconceptions About CDA Section 230*, HUFFINGTON POST (Feb. 17, 2014) ("The other, often overlooked goals of §230 include the development of technologies that "maximize user control over what information is received" by Internet users, as well as the "vigorous

Section 230, provided immunity from liability for 'Good Samaritan' online service providers that either over- or under-filtered objectionable content."[70] In other words, if online service providers' efforts are considered to be reasonable but ultimately come up short or go too far, they would be protected by Section 230. Thus, "[t]he idea was to incentivize—not penalize—private efforts to filter, block, or otherwise address noxious activity."[71] Section 230 protection was created to protect those platforms making "good faith" efforts to protect against dangerous content.

A year after the passing of Section 230, the case of *Zeran v. Am. Online, Inc.* ("AOL")[72] set the stage for application of the statute. Zeran, the plaintiff, sued AOL, arguing that it was negligent in failing to remove defamatory postings made by a third party.[73] In particular, Zeran argued that Section 230 allowed for liability for interactive computer services, like AOL, when they have notice of the defamatory postings distributed on their platforms.[74] The court dismissed Zeran's arguments, finding that treating AOL as a "distributor" would be essentially the same as treating it as a "publisher"—it would discourage online service providers from monitoring content, and thus, would be contrary to the purpose of Section 230.[75] "The court ignored the obvious point that Zeran's experience suggested that online intermediaries were already insufficiently motivated to address unlawful content."[76] That is, if the goal was to incentivize reasonable moderation practices, granting near-absolute immunity proved to do the opposite.

Zeran illustrates how Section 230 has *not* incentivized platforms to act in "good faith" or as "Good Samaritans," but instead has endorsed passive bystander-like conduct. Extending a duty, like that under a theory of premises liability, would motivate online service providers to address dangerous conditions present on their platforms. Instead, however, courts have interpreted Section 230(c)(1) as granting online service providers unfettered immunity from liability for content posted on their platforms by third parties—regardless of whether they were acting as what has been

---

enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking and harassment by means of computer." "In other words, the law is intended to promote and protect the values of privacy, security and liberty alongside the values of open discourse.").

70 Citron, *supra* note 67.

71 Citron & Franks, *supra* note 22 at 2.

72 *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997).

73 *Id.* at 328.

74 *Id.* at 331.

75 Franks, *supra* note 39.

76 *Id.*

traditionally defined as a publisher.[77] "[C]ourts have extended immunity from liability to platforms that republished content knowing it violated the law; solicited illegal content while ensuring that those responsible could not be identified; altered their user interface to ensure that criminals could not be caught; and sold dangerous products."[78]

However, a small minority of courts have denied Section 230 immunity to online intermediaries whose design features themselves have encouraged or facilitated illegal or unlawful content. The *Roommates.com* case is particularly worth noting because it is one of the few cases where a court has found that an online service provider cannot claim immunity under Section 230.[79] The Ninth Circuit used the concept of "neutral tools" to hold that Roommates.com was not entitled to Section 230 immunity for the operation of its system. Specifically, the court found that Roommates.com was designed to "steer users based on the preferences and personal characteristics that Roommate itself forces subscribers to disclose."[80] In its creation of such a system, Roommates.com acted as a content developer, not merely a publisher of third-party content, and was not immune under Section 230.[81]

The "Neutral Tools" concept is one method of analyzing Section 230 cases. In *Roommates.com,* the court distinguished features that could or could not be found to impose liability:

> If an individual uses an ordinary search engine to query for a 'white roommate,' the search engine has not contributed to any alleged unlawfulness in the individual's conduct; providing neutral tools to carry out

---

77 Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157, 1162-63. ("A website operator can be both a service provider and a content provider: If it passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content. But as to content that it creates itself, or is "responsible, in whole or in part" for creating or developing, the website is also a content provider. Thus, a website may be immune from liability for some of the content it displays to the public but be subject to liability for other content.").

78 Citron, *supra* note 71; *see* Shiamili v. Real Estate Group of New York, 17 N.Y.3d 281, 284-85 (N.Y. App Ct. 2011); Phan v. Pham, 182 Cal.App.4th 323, 325-26 (Cal. App. Ct. 2010); Jones v. Dirty World Entertainment Recordings, LLC, 755 F.3d 398, 401-02 (6th Cir. 2014); S.C. v. Dirty World, LLC, No. 11-CV-00392, 2012 WL 3335284, at *2 (W.D. Mo. March 12, 2012); *see, e.g.*, Hinton v. Amazon, 72 F. Supp. 3d 685, 687 (S.D. Miss. 2014).

79 *Fair Hous. Council of San Fernando Valley*, 521 F.3d at 1175; *see* Barnes v. Yahoo, 570 F.3d 1096, 1109 (9th Cir. 2009); F.T.C. v. Accusearch Inc., 570 F.3d 1187, 1201 (10th Cir. 2009); *see also* J.S. v. Village Media Holdings, LLC, 184 Wash.2d 95, 101-02 (Wash. S. Ct. 2015).

80 *Fair Hous. Council of San Fernando Valley*, 521 F.3d at 1167.

81 *Id.* at 1174.

> what may be unlawful or illicit searches does not amount to 'development' for purposes of the immunity exception.[82]

The distinction hinged on the provider's conduct[83]—whether the interactive computer service has created features that promote or openly allow misconduct, or whether the service provider's neutral features are simply being used for wrongdoing.[84] Ultimately, the Ninth Circuit reasoned that the site's drop down menu, which required subscribers to indicate preferences in "sex, sexual orientation, and whether he has children . . . ," was *created* by Roommates.com.[85] Contrarily, the Ninth Circuit concluded that Section 230 immunity applied to the free form space for "Additional Comments", where users could freely write their preferences or whatever else they may want, without any choice given by the website because the information included was the user's own publication.[86]

However, this "neutral tools" analysis is only one method courts have used to distinguish when an online entity is acting as an interactive computer service or an information content provider.[87] Applying the theory of premises liability, the Court would have concluded that Roommates.com was not immune from liability because it was reasonably foreseeable that the drop-down menu (and "Additional Comments" space) would be used for discriminatory purposes. This analysis would have set a standard for future online liability cases: Online operators must implement reasonable content moderation practices in light of foreseeable harm to be extended Section 230 immunity. Unfortunately, this was not the case and the Court's holding has proved to be extremely narrow.

For example, in *Doe IX v. Myspace, Inc.*, plaintiff argued under the same theory used in *Roommates.com* that "[d]efendant [was] an information content provider because it developed the information on the

---

82 *Id.* at 1169.

83 42 U.S.C. § 230(f)(2).

84 *Fair Hous. Council of San Fernando Valley*, 521 F.3d at 1171 (citing to Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003), stating that there, the website provided neutral tools which the anonymous user used to publish libel, but the website did nothing to encourage, thus, the website operator could not be held liable).

85 *Id.* at 1165.

86 *Id.* at 1166.

87 *See id.* at 1169 (emphasizing that neutral tools do not contribute to the unlawfulness of the third-party's conduct—for example, here, a blank space allowing users to input specific information that may be discriminatory but does not contribute to that, while on the other hand the drop-down menu, which specified discriminatory criteria for a roommate, did contribute to the unlawfulness of the conduct).

profiles which caused [the plaintiff's] injuries."[88] The court found that *Roommates.com* was distinguishable because it required users to provide specific information, while Myspace merely allowed for additional information to be added.[89] Furthermore, in *Jones v. Dirty World Entertainment Recordings, LLC*, immunity was once again extended to a defendant whose website was created for the primary purpose of posting gossip about public figures.[90] TheDirty would select and publish user submissions with small blurbs describing the content.[91] Despite this, the court found that the defendant did not *create* content and therefore, was immune from liability.[92]

However, in *Doe v. Internet Brands, Inc.* (d/b/a ModelMayhem.com) (hereinafter "Model Mayhem"), the Ninth Circuit upheld the plaintiff's failure to warn claim.[93] The plaintiff, an amateur model, used Model Mayhem, a networking site for people in the modeling industry, where she was lured to a fake audition, drugged, raped, and recorded for a pornographic video.[94] She alleged that Model Mayhem knew of the rape scheme, because the individuals involved had been criminally charged, and should thus be responsible for failing to warn her of the danger.[95] The Ninth Circuit held that the plaintiff's claim was not precluded by Section 230 because she was not "seek[ing] to hold Internet Brands liable as the 'publisher or speaker of any information provided by another information content provider.'"[96] Instead, the plaintiff sought to hold Model Mayhem liable for failure to warn—she was not seeking to hold Model Mayhem liable for the conduct of third-parties but for its lack of response to that conduct. Likewise, under a theory of premises liability, the plaintiffs would not seek hold online intermediaries liable under traditional publisher liability, but seek to hold them liable for their failure to exercise "good faith" content moderation practices. Under the theory of premises liability, "good faith" content moderation practices would be interpreted to mean those that are *reasonable* in light of the *foreseeable harm*.

Another approach was that taken by the court in *Jane Doe No. 1 v. Backpage.com LLC* ("Backpage"), where the plaintiffs sued Backpage, claiming that as minors they were victims of sex-trafficking via the

---

88 Doe IX v. Myspace, Inc., 629 F.Supp.2d 663, 665 (Dist. Ct. E.D. Tex. 2009).
89 *Id.* at 665.
90 Jones v. Dirty World Entertainment Recordings LLC, 755 F.3d 398, 402 (6th Cir. 2014).
91 *Id.* at 401.
92 *Id.*
93 Doe v. Internet Brands, Inc., 824 F.3d 846, 854 (9th Cir. 2016).
94 *Id.* at 848.
95 *Id.* at 849.
96 *Id.* at 851.

defendant's website.[97] The plaintiffs alleged that Backpage facilitated sex-trafficking by third-party users.[98] Further, the plaintiffs argued that Backpage deliberately created its website to encourage sex trafficking, or at a minimum make it easier. Specifically, although Backpage filtered out some prohibited terms, it did not filter out known substitutes—for example, "barely legal" was prohibited but "brly legal" was not.[99] Through its allowance of anonymity, code terminology used to refer to sexual services by underage girls, and altered telephone numbers, Backpage was a hub for sex trafficking. Despite these facts, the court found that Section 230 immunity was to be applied broadly and extended to Backpage.[100]

Following *Backpage.com*, President Donald Trump signed into law a pair of bills, the "Fight Online Sex-Trafficking Act" ("FOSTA") and "Stop Enabling Sex-Traffickers Act" ("SESTA")—together known as FOSTA-SESTA.[101] The bills created an exception to Section 230, making websites responsible for postings made "with the intent to promote or facilitate the prostitution of another person . . . ."[102] Thus, the bills "created additional criminal and civil liability for sex trafficking"[103] and were specifically intended to combat the kind of sex-trafficking activity taking place on Backpage.[104] It is important to note that sex trafficking, as a violation of federal criminal law, was already an exception to Section 230 immunity.[105] But FOSTA-SESTA gave prosecutors "greater power to pursue websites that host sex-trafficking ads and enables victims and state attorneys general to file lawsuits against those sites."[106]

Although the passing of the bills was seemingly a win for society, this piecemeal approach is unlikely to be successful in the long run. Immunity for online actors affects plaintiffs in several contexts including, but not

---

97 *See* Jane Doe No. 1 v. Backpage.com LLC*,* 817 F.3d 12, 16 (1st Cir. 2016).

98 *Id.* at 19.

99 *Id.* at 16-17.

100 *Id.* at 19.

101 Aja Romano, *A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as we Know It,* VOX, (Jul. 2, 2018), https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom.

102 *Id.* (quoting H.R. 1865 - Allow States and Victims to Fight Online Sex Trafficking Act of 2017).

103 Jennifer Huddleston Skees, *A Cautionary Tale on Internet Freedom Carve-Outs*, THE HILL (Jan. 17, 2019), https://thehill.com/opinion/technology/425768-a-cautionary-tale-on-internet-freedom-carve-outs.

104 Romano, *supra* note 101.

105 47 U.S.C. § 230(e)(1) (2018).

106 Tom Jackman, *Trump Signs 'FOSTA' Bill Targeting Online Sex Trafficking, Enables States and Victims to Pursue Websites*, WASHINGTON POST (April 11, 2018) https://www.washingtonpost.com/news/true-crime/wp/2018/04/11/trump-signs-fosta-bill-targeting-online-sex-trafficking-enables-states-and-victims-to-pursue-websites/.

limited to, nonconsensual pornography ("revenge porn"), terrorism, defamation, discrimination, harassment, fraud and misrepresentation in online dating, and illegal transactions of firearms.[107] Therefore, addressing Section 230 immunity one context at a time would prolong the fight and result in the continuous posting of dangerous content online, which—as can be seen from the abundance of case law surrounding Section 230 immunity—has resulted in devastating consequences for plaintiffs and users generally. The growth of the Internet makes it almost impossible to reliably predict new contexts where Section 230 may arise and result in harmful consequences in the future. Contrarily, under the theory of premises liability, by extending a duty of care to online service providers, courts could reach outcomes that adhere to the goal of Section 230 to incentivize online service providers, abide by classical tort principles long accepted in physical spaces, and set precedent for future cases.[108]

III. PREMISES LIABILITY

Premises liability is a type of negligence claim where a plaintiff alleges that his or her injuries or damages were a result of the defendant's failure to maintain the premises he or she operates in a "reasonably safe condition".[109] For a plaintiff to successfully sue under the theory of premises liability, he or she must typically demonstrate (1) that he or she was legally present on the land, meaning that he or she was not trespassing; and (2) that the defendant had a duty to protect against his or her injuries or damages (a) because the defendant knew or should have known that there was a dangerous condition and (b) should have expected that the plaintiff would fail to protect against said condition.[110] The plaintiff must also demonstrate that the defendant's conduct—his or her failure to

---

[107] *See* Zak Franklin, *Justice for Revenge Porn Victims: Legal Theories to Overcome Claims of Civil Immunity by Operators of Revenge Porn Websites*, 102 CAL. L. REV. 5 (2014); *see* Cohen v. Facebook, 252 F. Supp.3d 140, 146-47 (Dist. Ct. E.D. N.Y. 2017); Jones v. Dirty World Entertainment Recordings LLC, 755 F.3d 398, 401-02 (8th Cir. 2014); Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157, 1161-62 (9th Cir. 2008).; Herrick v. Grindr, LLC, 306 F.Supp.3d 579, 584 (S.D. N.Y. 2018); Daniel v. Armslist, LLC, 386 Wis.2d 449, 457 (Wis. 2019).

[108] *See* Kim, *supra* note 20 at 1012 ("Online harassment can be combatted by changing the roles the Web site sponsors currently play and by imposing tort liability on those who fail to meet certain expectations. Web site sponsors maintain a proprietary interest in their Web sites, and we should expect them to conform to the standard of conduct expected of other proprietors.")

[109] Ann M. v. Pac. Plaza Shopping Ctr., 6 Cal. 4th 666, 674 (stating that under a theory of premises liability, a plaintiff alleges that a defendant did not "[m]aintain land in their possession and control in a reasonably safe condition.").

[110] RESTATEMENT (SECOND) OF TORTS § 343 (1965).

exercise reasonable care—was the cause of his or her injuries.[111] Typically, the determination of whether a duty exists turns on the foreseeability of the danger.[112] Under this theory, a duty to take reasonable precautionary or protective measures has been found to extend to land operators that open their premises up to the public, even for conduct committed by third parties.[113]

A. History of Premises Liability

Under the common law system, premises liability cases turned on the landowner's relationship to the visitor.[114] A landowner owes the highest duty of care to invitees.[115] "Since the invitee has been invited onto the land by the landowner, whether implicitly or explicitly, the landowner has a duty of 'reasonable care for his safety.'"[116] This duty to invitees required landowners to warn them of potentially dangerous conditions and protect against dangers the owner knows or has reason to know may result in harm.[117] The second category is that of the licensee, which is "a 'person who is privileged to enter or remain on the land only by virtue of the possessor's consent.'"[118] Essentially, the duty a landowner owes to licensees is that of reasonable care for dangers the individual is unlikely to know about and protect against.[119] The last category is that of a trespasser, which is someone "'who enters or remains on the land in possession of another without a privilege to do so . . . .'"[120] Typically, landowners have no affirmative duty to protect trespassers.[121]

In the beginning of the twentieth century, the importance of these categories for visitors diminished.[122] In *Rowland v. Christian*, the California Supreme Court held that premises liability would depend on whether the landowner acted reasonably "'in view of the probability of

---

111 *Id.*

112 *See* Wylie Clarkson, *Premises Liability in South Carolina: Should You Expect Criminal Activity On Your Property?*, 3 CHARLESTON L. REV. 619, 619 (2009); W. Marshall Sanders, *Between Bystander and Insurer: Locating the Duty of Georgia Landowner to Safeguard Against Third-Party Criminal Attacks on the Premises*, 15 GA. ST. U. L. REV. 1099, 1108 (1999).

113 *See* Martin v. Rite Aid of Pa, Inc., 80 A.3d 813, 815 (2013) ("[P]ossessors of land who hold it open to the public . . . owe a duty to any business invitee . . . to take reasonable precaution against harmful third-party conduct that might be reasonably anticipated.").

114 Driscoll, *supra* note 32 at 883.

115 *Id.*

116 *Id.*

117 *Id.*

118 *Id.*

119 *Id.* at 884.

120 *Id.*

121 *Id.*

122 *Id.* at 885.

injury to others,' while the plaintiff's status as a licensee, invitee, or trespasser would be only one factor in the liability inquiry and no longer controlling in any case."[123] Numerous state courts followed the decision to abandon the categorical approach to premises liability following *Rowland.*[124] While many jurisdictions have abandoned the approach completely, a near majority continue to use it.[125] Some other jurisdictions have decided to keep the trespasser category but merge the licensee and invitee categories.[126]

The law of premises liability remains unsettled and depends on the jurisdiction.[127] Nonetheless, core concepts of premises liability can be applicable to virtual spaces as well as physical spaces. Typically, website operators "implicitly or explicitly" invite users onto their property.[128] Thus, users can be categorized as invitees. Even if users are not found to be invitees, they *cannot* be categorized as trespassers because website operators generally either open their platforms up to the public or consent to users being present on their websites by requiring the creation of an account, for example. Despite the fact that websites are not physical property, the domains are owned and operated in similar ways to physical property. As such, the theory of premises liability is applicable to virtual spaces owned and operated by online intermediaries. Part IV of this note will detail the theory's applicability to the online context.

B. Premises Liability and Third-Party Criminal Acts

Of specific importance in applying the theory of premises liability to the online context is the imposition of liability on landowners for harms caused by the unlawful acts of third parties. Historically, courts were disinclined to impose a duty on landowners to protect against third-party conduct because of difficulty in finding proximate causation.[129] However, the duty under the theory of premises liability extends to landowners when the potential harm from third-party conduct is reasonably foreseeable.[130]

---

123 *Id.* at 887 (citing to *Rowland v. Christian,* 443 P.2d 561 (Cal. 1968)).

124 *Id.* at 888.

125 *Id.* at 890 ("A near majority of states have actually rejected a unitary standard and still apply the tripartite system").

126 *Id.* ("Further, many state courts have preserved the trespasser distinction while merging licensee and invitee into one category").

127 *Id.*

128 *See id.* at 883.

129 W. Marshall Sanders, *Between Bystander and Insurer: Locating the Duty of Georgia Landowner to Safeguard Against Third-Party Criminal Attacks on the Premises*, 15 GA. ST. U. L. REV. 1099, 1102 (1999).

130 RESTATEMENT (SECOND) OF TORTS § 344 cmt. f. (1965) ("If the place or character of his business, or his past experience, is such that [a possessor of land] should reasonably

In *Kline v. 1500 Massachusetts Avenue Apartment Corp.*, the court extended liability to the landowner of an apartment building for the injuries the plaintiff sustained after being assaulted and robbed in the apartment complex hallway.[131] The court reasoned that the landowner had a duty to provide protection because he "possess[ed] both superior knowledge and resources to safeguard against [the] criminal attack."[132] Specifically, the landlord knew of the increased number of "assaults, larcenies, and robberies" which occurred after the decision to leave the building's entrances unguarded.[133] Likewise, in the online context, interactive computer service providers possess the knowledge and resources to be able to protect users, and others, from crimes occurring on, or facilitated by their websites—as is evident by the examples set forth in Part II and which will be further discussed in Part IV.[134]

Premises liability has been successfully invoked for physical harm and emotional / mental harm, also known as pain and suffering.[135] For example, tort law has been successfully invoked to compensate a witness of a violent act suffering from post-traumatic stress disorder, as well as, a plaintiff suffering from emotional distress due to harassment.[136] Generally, tort law serves two purposes to (1) compensate plaintiff's for the harm they have suffered and (2) deter future negligent conduct. Similarly, the tort law principles at the core of the theory of premises liability should be extended to the online context for the purpose of remedying victims' harms and incentivizing website operators to make "good faith" efforts to protect against conduct that results in an unlawful or dangerous condition, that is foreseeably likely to result in harm. There are four approaches for determining whether harm (physical or non-physical) is foreseeable: the specific imminent harm approach, the prior similar incidents approach, the

---

anticipate carless or criminal conduct on the part of third persons, either generally or at some particular time, he may be under a duty to take precautions against it . . . .").

131 Sanders, *supra* note 129 at 1099.

132 *Id.* at 1105.

133 Kline v. 1500 Mass. Ave. Apt. Corp., 439 F.2d 477, 479 (D.C. App. Ct. 1970).

134 *See* Zeran v. Am. Online, Inc., 129 F. 3d 327, 327 (4th Cir. 1997); Doe IX v. Myspace, Inc. 629 F.Supp.2d 663, 663 (E.D. Tex. 2009); Jones v. Dirty World Entertainment Recordings LLC, 755 F.3d 398, 402 (6th Cir. 2014); Jane Doe No. 1 v. Backpage.com LLC, 817 F.3d 12, 12 (1st Cir. 2016); *see also* Herrick v. Grindr, LLC., 306 F.Supp.3d 579, 579 (S.D. N.Y. 2018); Daniel v. Armslist, LLC, 386 Wis.2d 449, 449 (Wis. 2019); Kim, *supra* note 20 at 1035 ("Web site sponsors maintain control over the content of the site . . . and are in the best position to prevent harm to other users on the site.").

135 RESTATEMENT (SECOND) OF TORTS § 343 (1965).

136 *See* Greene v. Young, 113 Wash.App. 746, 748 (Wash. App. Ct. 2002); Henrickson v. State, 319 Mont. 307, 312, 84 P. 3d 38, 44-45 (Mont. 2004); *see* Blakey v. Continental Airlines, Inc., 992 F.Supp. 731, 733-34 (N.J. Dist. Ct. 1998); Coleman v. Tennessee, 998 F.Supp. 840, 843 (Tenn. Dist. Ct. 1998).

totality of the circumstances approach, and the balancing approach.[137] Which approach will be used to determine foreseeable harm depends on the jurisdiction.[138]

Under the specific imminent harm approach, the most restrictive approach, landowners have a duty of care when they "know or have reason to know" that there is conduct occurring or about to occur that poses "imminent probability of harm."[139] The specific imminent harm approach requires that specific evidence that a particular harm was imminent and that the landowner knew that it was imminent.[140] This approach is unlikely to fare well in the online context because of the specificity and imminence requirements. However, for example, in the case of *Herrick v. Grindr*, Herrick repeatedly reported the harassment and abuse he was experiencing to Grindr.[141] Despite this, Grindr did absolutely nothing to rectify these dangerous conditions.[142] As such, it could be argued that in cases where multiple reports are made to the online service provider, the providers know or have reason to know that the conduct is likely to lead to the specific harm complained of.

The prior similar incidents approach requires a plaintiff show that "prior crimes [occurred] on or near the owner's property."[143] Under this approach, cases are decided on a case-by-case basis[144]—the landowner has a duty to protect against and anticipate harm based on the fact that a similar crimes have occurred before. This approach would only hold online intermediaries liable after a similar crime occurred on the platform. However, the theory of premises liability wants to encourage online service providers to foresee potential consequences of the features on their platform and engage in reasonable content moderation practices *before* harm occurs. Additionally, this approach might not succeed in the online context because the breadth of the internet allows for various distinctive

---

137 *See* Clarkson, *supra* note 112 at 619-621.

138 *See id.* at 619.

139 *Id.* at 621. ("In other words, the injured party is required to prove that the property owner knew of the specific imminent harm which was about to occur.").

140 *Id.*

141 Herrick v. Grindr, LLC, 765 F. App'x 586 (2d Cir. 2019), *petition for cert. filed,* (U.S. Aug. 7, 2019) (No. 19-192) ("Between November 2016 and January 2017, Herrick reported Grindr's targeting of him and his stalking approximately fifty times to Grindr.").

142 *Id.* at 10.

143 Clarkson, *supra* note 112 at 621; *see* 1 JOHN ELLIOTT LEIGHTON, LITIGATING PREMISES SECURITY CASES (West ed., 6th ed. 2020) ("[T]he plaintiff needs to show that based on prior similar incidents, it was likely that a patron of the defendant's establishment, without defendant's precautions to prevent it, would be injured by the criminal act of a third person.").

144 Clarkson, *supra* note 112, at 622, 623.

crimes to be carried out in different ways so online intermediaries may more easily escape liability on a narrow distinction or technicality.

Under the totality of the circumstances approach, "courts consider all of the circumstances surrounding the criminal act and the 'nature, condition, and location of the premises, in addition to any prior similar incidents, and a duty can be found where no prior criminal attacks have occurred.'"[145] This approach has been found to be extremely burdensome on businesses because it requires them to potentially protect against random criminal acts by others.[146]

The final approach is the balancing approach, which "'weighs the foreseeability of the harm against the burden imposed on a [landowner] by protecting against that harm.'"[147] In order for a duty to be extended to landowners, the foreseeability of the harm must outweigh the burden of taking precautionary or protective measures.[148] This approach aims to find a balance between an injured party's rights and a business's economic interests.[149] "The balancing approach acknowledges that duty is a flexible concept, and seeks to balance the degree of foreseeability of harm against the burden of duty imposed. As such, the more foreseeable a crime, the more onerous the business owner's burden of providing security."[150]

In summary, under the theory of premises liability, a defendant will only be found liable if the plaintiff can show: (1) that the defendant had a duty to protect against foreseeable harm, and (2) that the defendant's actions, or failure to take action, resulted in his or her injuries or damages. In other words, the plaintiff must demonstrate how the defendant's decision to forego certain protective or remedial measures were the proximate cause of his or her injuries or damages.[151] The same duty should

---

145 *Id.* at 625.

146 *Id.* at 626. ("[T]he test is too broad and imposes 'an unqualified duty to protect customers in areas experiencing any significant level of criminal activity.' Additionally, the test has been considered and found to be 'too broad and unpredictable, effectively . . . requiring landowners [to] anticipate crime.'").

147 *Id.* at 627.

148 *Id.* ("'[T]he degree of foreseeability needed to establish a duty decreases in proportion to the magnitude of the foreseeable harm' and the burden upon defendant to engage in alternative conduct.").

149 *Id.* at 629. (This approach has been compared to the 'Hand Formula' which "essentially defines negligence as the unreasonable balancing of the cost of safety measures against the risk of accidents.").

150 Robert W. Foster, et al., *Balancing Act: Does a South Carolina Property Owner Have a Duty to Protect its Invitees from Third-Party Crime?*, NELSON MULLINS, 27 (2011), https://www.nelsonmullins.com/storage/33daeb28a85b7e2722c9ac2cc23c301b.pdf.

151 Nallan v. Helmsley-Spear, Inc., 407 N.E.2d 451, 459 (N.Y. 1980) ("[T]he fact that the 'instrumentality' which produced the injury was the criminal conduct of a third person would not preclude a finding of 'proximate cause' if the intervening agency was itself a foreseeable hazard'").

be extended to website operators in the online context. As previously mentioned, this duty would not require online service providers to protect against any and all harm, but only against conduct that is foreseeably likely to result in harm[152] This theory would hold online operators responsible for the decisions made in respect to their website, and thus, incentivize them to make "good faith" efforts to moderate foreseeably dangerous conduct.

IV. PREMISES LIABILITY IN THE ONLINE CONTEXT

As previously mentioned, a premises owner or operator is not always liable for conduct of a third party.[153] However, the duty under the theory of premises liability extends to landowners when the potential harm from third-party conduct is reasonably foreseeable.[154] This note focuses on the duty that should be extended to online service providers and the causation requirement that must be established for a successful premises liability claim in the online context.

It is first important to note and distinguish the *reasonable* content moderation approach proposed by Danielle Keats Citron and Benjamin Wittes in 2018 from what is being suggested here.[155] The interpretive shift proposed by Citron and Wittes is similar to the approach outlined in this note. First, as stated by Citron and Wittes, courts should not apply Section 230 immunity unless the plaintiff's claims relate to the *publication* of third-party content.[156] Essentially, courts should *only* extend Section 230 immunity to platforms when the plaintiffs in those cases attempt to hold them liable as "publishers" or "speakers" of third-party content.[157] Second, Citron and Wittes argue that courts should limit Section 230 immunity to those platforms that act as "Good Samaritans."[158] A "Good Samaritan" is one who "take[s] reasonable steps, when warned, to protect against illegal

---

152 *See* Michael L. Rustad and Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L. J. 1553, 1584 (2005) ("A court using [the balancing test] would look at all relevant circumstances, including the number, nature, and location of prior similar computer crimes and the closeness of the connection between defective software and the intrusions.").

153 Clarkson, *supra* note 112 at 619.

154 RESTATEMENT (SECOND) OF TORTS § 344 cmt. f. (1965) ("If the place or character of his business, or his past experience, is such that [a possessor of land] should reasonably anticipate carless or criminal conduct on the part of third persons, either generally or at some particular time, he may be under a duty to take precautions against it . . . .").

155 Citron & Wittes, *supra* note 14 at 456.

156 *Id.* at 467.

157 *Id.* at 468.

158 *Id.*

activity or that proactively address[es] illegal material . . . but end[s] up under-screening."[159]

The premises liability analysis proposed in this note ultimately aims to achieve the same goals as Citron and Wittes' *reasonable* content moderation proposal.[160] However, analysis under the theory of premises liability is an application of a distinct theoretical framework based on classical tort principles. Under a theory of premises liability, courts can adhere to the distinction between a publisher and another tortfeasor—principally, a landowner who failed to take reasonable precautionary measures in light of potential harm.

This section will apply premises liability concepts to the cases of *Herrick v. Grindr* and *Daniel v. Armslist*, the plaintiffs in which both petitioned, unsuccessfully, the U.S. Supreme Court for review in 2019. Before applying the theory of premises liability to those cases, this section summarizes the cases' factual background, procedural history, holdings, and reasoning.

A. Summary of Herrick v. Grindr[161]

Matthew Herrick ("Plaintiff" or "Herrick"), filed suit against Grindr, LLC ("Defendant" or "Grindr"), alleging products liability, negligent design, promissory estoppel, fraud, and copyright infringement.[162] Herrick is a former user of the Defendant's dating application, Grindr. The Defendant is characterized as an internet service provider under Section 230. Grindr maintained a dating application for gay and bi-sexual individuals. Herrick's former boyfriend used Grindr to harass Herrick and subject him to "malicious catfishing" by using available features on the application.[163]

Like other dating apps, Grindr requires users to set up a profile by inputting their email address and other information, such as the user's name, photographs, and information about themselves.[164] Grindr then uses an algorithm based on the users' sexual preferences and location to allow matching.[165] Once two users have matched they can send each other

---

159 *Id.*

160 *See id.* at 467-68.

161 *See* Carrie Goldberg, Herrick v. Grindr*: Why Section 230 of the Communications Decency Act Must Be Fixed,* LAWFARE (Aug 14, 2019, 8:00 AM), https://www.lawfareblog.com/herrick-v-grindr-why-section-230-communications-decency-act-must-be-fixed.

162 Herrick v. Grindr, LLC, 306 F. Supp. 3d 579, 579 (S.D.N.Y. 2018).

163 *Id.* at 584.

164 *Id.*

165 *Id.*

messages and share location data with each other.[166] Matthew Herrick and his ex-boyfriend matched on Grindr and began an exclusive relationship in 2015, upon which Herrick deleted the application.[167]

Upon their separation, Herrick's ex-boyfriend used Grindr to impersonate Herrick by posting fake profiles stating that Herrick was interested in rough sexual encounters, including rape fantasies and bondage.[168] Despite Herrick's numerous reports to Grindr complaining of the profiles impersonating him, Grindr failed to substantively respond.[169] As a result, hundreds of Grindr users who matched with the impostor profiles of Herrick sought him out—approximately 1,100 users.[170] Grindr's direct messaging and geolocation features were used by Herrick's ex-boyfriend to harass and harm Herrick.[171] "Users were transmitted maps of Herrick's location, and some of the men were told to expect that Herrick would resist their approach, which they were told was part of a rape-fantasy or roleplay."[172]

Herrick argued that Grindr's application design choices enabled the continued harassment he experienced.[173] Herrick alleged that Grindr failed to "incorporate certain safety features that could prevent impersonating profiles."[174] Grindr could have implemented the use of "common image recognition or duplicate-detection software" to find and remove impersonating profiles.[175]

Moreover, Grindr neither uses keyword search functions in its direct messaging feature nor does it have the capability to "search for IP addresses, MAC addresses, and ICC numbers or block the use of spoofing, proxies, and virtual private networks (VPN's)", which could be easily implemented.[176] Grindr also failed to use "geofencing" which would have allowed Grindr to discover whether an account was associated with Herrick's address or his ex-boyfriend's address.[177] Herrick also argued that Grindr had sufficient notice of the misuse, and potential future misuse, occurring on its application because he had filed multiple reports regarding the accounts, and still failed to warn users.[178] Despite this knowledge,

---

166 *Id.*
167 *Id.* at 584-85.
168 *Id.*
169 *Id.* at 585.
170 *Id.*
171 *Id.*
172 *Id.* (referring to allegations in Plaintiff's Amended Complaint ¶52 and ¶62).
173 *Id.*
174 *Id.*
175 *Id.*
176 *Id.* at 585.
177 *Id.*
178 *Id.*

Grindr led users to believe that it had security measures in place to prevent harassment and that it valued the safety of its users.[179] Grindr designed its dating application in a manner that allowed it to be "easily manipulated and misused" and failed to take reasonable precautions to prevent, or rectify, potentially dangerous conditions.[180] This made it possible for Herrick's ex-boyfriend's to facilitate criminal and intentionally tortious conduct through the Grindr app.

Grindr successfully sought to cloak itself with the broad immunity consistently granted by courts under Section 230 of the CDA. Grindr argued that holding it responsible for failing to remove or block the impersonating profiles would be to find it responsible for acting as a publisher of third-party content, as prohibited by Section 230.[181] The District Court for the Southern District of New York held that Grindr was entitled to immunity under the CDA and granted Grindr's motion to dismiss.[182] "To the extent Herrick has identified a defect in Grindr's design or manufacture or a failure to warn, it is inextricably related to Grindr's role in editing or removing offensive content—precisely the role for which Section 230 provides immunity."[183] The United States Court of Appeals for the Second Circuit affirmed the decision,[184] echoing the District Court that Herrick's "manufacturing and design defect claims seek to hold Grindr liable for its failure to combat or remove offensive third-party content, and are barred by § 230."[185] In his last hopeful effort, Matthew Herrick petitioned the Supreme Court of the United States for a writ of certiorari.[186] The Supreme Court denied Herrick's petition on October 7, 2019.[187]

Cases challenging the application of Section 230's immunity provision, like *Herrick v. Grindr*, are frequently dismissed prior to the discovery phase. In approximately 92% of cases where the Section 230 immunity defense is advanced, the courts will address it (and oftentimes

---

179 *Id.* at 586.
180 *Id.*
181 *Id.* at 587.
182 *See id.*
183 *Id.* at 588.
184 *See* Herrick v. Grindr, LLC, 765 Fed.Appx. 586, 593 (2d Cir. 2019).
185 *Id.* at 590; *see* Jane Doe No. 1 v. Backpage.com, LLC, 817 F.3d 12, 21 (1st Cir. 2016) (claims based on the "structure and operation" of a defendant ICS were barred by § 230 because the lack of safety features reflects "choices about what content can appear on the website and in what form," which are "editorial choices that fall within the purview of traditional publisher functions").
186 *See* Herrick v. Grindr, LLC*,* 765 F. App'x 586 (2d Cir. 2019), *petition for cert. filed,* (U.S. Aug. 7, 2019) (No. 19-192).
187 Order Denying the Petition for Writ of Certiorari, 140 S. Ct. 221 (2019).

dismiss the cases) prior to discovery.[188] The decision to forgo discovery not only prevents plaintiffs from bringing their legitimate claims against online operators and learning of their content moderation practices, but it also prevents online service providers from improving their operations by learning of the potentially dangerous features on their platform. As such, online operators are not incentivized or given the opportunity to discover new technologies or techniques that could increase user safety, and thus, promote growth. For example, female users may be more inclined to use a social media platform or dating application, if they believe that the online service provider is engaging in reasonable content moderation that protects users from fake accounts or threats. Discovery of reasonable content moderation will expand the marketplace of ideas by encouraging users, primarily minorities, to engage on those platforms implementing those practices.

This lack of safety contradicts Section 230's stated goal of promoting a free marketplace of ideas because it discourages individuals from speaking out of fear of harassment. Interactive computer service providers are granted total immunity without even the threat of potential discovery that could reveal an unreasonable lack of safety measures.[189] Just as landowners or businesses are encouraged to discover adopt safety features in physical spaces, especially after harmful incidents, so could the owners and operators of the online spaces.[190] Without access to discovery, plaintiffs are excluded from the opportunity of arguing that the online platform failed to act in "good faith" and online service providers are

---

[188] David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 483 (2010) ("A court refused to address the defendant's section 230 defense prior to discovery in only 7.6% of the decisions.").

[189] Carrie Goldberg, Herrick v. Grindr*: Why Section 230 of the Communications Decency Act Must be Fixed,* LAWFARE, https://www.lawfareblog.com/herrick-v-grindr-why-section-230-communications-decency-act-must-be-fixed (August 14, 2019) ("There are, or should be, fact-intensive inquiries, but if cases are dismissed on motions to dismiss for failure to state a claim, as ours was—before discovery and without defendants even needing to plead Section 230 immunity—plaintiffs will never have a chance.").

[190] *See* Citron & Wittes, *supra* note 45 at 403 ("In physical space, a business that arranged private rooms for strangers to meet, knowing that sexual predators were using its services 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 (referring to Omegle.com). 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.").

discouraged from discovering what would constitute "good faith" practices, those that are reasonable in light of the foreseeable harm.

B. Summary of Daniel v. Armslist

Yasmeen Daniel ("Plaintiff" or "Daniel"), brought a series of tort actions on behalf of herself and her deceased mother, Zina Daniel Haughton ("Zina") against Armslist LLC ("Defendant" or "Armslist").[191] Radcliffe Haughton ("Haughton"), was the victim's estranged husband who used the Defendant's website to purchase a firearm and murder Zina in front of her daughter.[192] Armslist is characterized as an interactive computer service provider under Section 230. Armslist is an online marketplace that facilitates firearm transactions by third-party buyers and sellers.[193] Houghton utilized Armslist.com to illegally purchase the weapon that resulted in the demise of Plaintiff's mother, Zina.[194]

In October 2012, a Wisconsin court granted Zina a restraining order against her husband, Haughton, after a domestic violence dispute.[195] The terms of the order prohibited Haughton from possessing a firearm.[196] Nevertheless, Haughton visited Armslist.com and arranged the purchase of a semiautomatic handgun from a third party.[197] On October 21st, a day after acquiring the firearm, Haughton went to the salon where Zina worked, killed three people, injured four others, and then shot himself.[198] Daniel was in the salon at the time of the shooting and witnessed the tragic events described.[199] Daniel brought several tort claims against Armslist, alleging that Armslist facilitated the illegal purchase of a firearm that Houghton would have otherwise had difficulty obtaining.[200] In facilitating and expediting Houghton's illegal purchase of a firearm, Armslist essentially removed Zina's sole source of protection.

Daniel alleged that Haughton specifically relied on the Defendant's website, Armslist.com, to purchase the firearm used in the brutal event resulting in this case.[201] Armslist utilized several design features that made it easy for individuals prohibited from purchasing, carrying, or using firearms to acquire one anyway. Armslist did not require purchasers or

---

191 Daniel v. Armslist, LLC, 386 Wis.2d 449, 449 (Wis. 2019).
192 *Id.* at 459.
193 *Id.* at 457.
194 *Id.* at 458.
195 *Id.* at 458-59.
196 *Id.* at 459.
197 *Id.*
198 *Id.*
199 *Id.*
200 *Id.* at 449.
201 *Id.* at 460.

sellers to register accounts and allowed them to maintain anonymity.[202] Armslist's features allowed people with court mandated firearms restrictions, as the case at hand, not only to illegally purchase a firearm, but to avoid requirements like state-mandated waiting periods.[203]

Furthermore, Armslist allowed potential purchasers to filter private sellers from federally licensed gun dealers.[204] This further simplified illegal firearm sales because private sellers are not required to conduct background checks that could reveal possible reasons for preventing a particular sale.[205] Although Armslist did in fact have a flagging component on its website, which is generally a positive step for website operators in restricting harmful conduct, the feature did not apply to illegal conduct but rather only to "spam," "miscategorized," or "overpriced" postings, or those similar in nature.[206] As such, Armslist gave a simple means for purchasing firearms to those whom access was intended to be most restricted.

"Based on all these features and omissions, Daniel's complaint alleged that Armslist knew or should have known that its website would put firearms in the hands of dangerous, prohibited purchasers, and that Armslist specifically designed its website to facilitate illegal transactions."[207] Daniel argued that her suit did not seek to treat Armslist as a publisher, but to hold it responsible for "the design and operation of its website, [which] helped to develop the content of the firearm advertisement".[208] Daniel based her claims on Armslist's "facilitation and encouragement of illegal firearm sales by third parties," not on the content specifically posted by the third-party seller.[209] Armslist countered that it was immune as an interactive computer service provider under Section 230.[210]

In this case, the Supreme Court of Wisconsin applied the Material Contribution Test to determine whether a computer service provider is immune from liability.[211] The Material Contribution Test is one method of analysis used to aid courts in determining when an interactive computer service provider is acting as an information content provider.[212] The Test sates that if the website contributes materially to the alleged illegal

---

202 *Id.*
203 *Id.*
204 *Id.*
205 *Id.* at 475.
206 *Id.* at 460.
207 *Id.* at 461.
208 *Id.* at 466.
209 *Id.* at 466-67.
210 *Id.* at 467.
211 *Id.* at 468.
212 *See id.* at 467-68 (discussing why courts use the "material contribution" test).

conduct, the website can be seen as a developer of that content.[213] However, a site cannot be liable for merely displaying the allegedly illegal conduct.[214] Additionally, the Court looked at the concept of "neutral tools" to determine whether the design features were a material contribution to the illegal conduct or content.[215] As previously discussed in Part II, "[a] 'neutral tool' in the CDA context is a feature provided by an interactive computer service provider that can 'be utilized for proper or improper purposes.'"[216] In *Roommates.com*, the Ninth Circuit distinguished "neutral tools" by looking at the potential for lawful use of the tool.[217] "[I]f a website's design features can be used for lawful purposes the CDA immunizes the website operator from liability when third parties use them for unlawful purposes."[218]

The Circuit Court dismissed Daniel's action, finding that Section 230 of the CDA barred her claims.[219] The Court of Appeals of Wisconsin reversed the lower court's decision, holding that because Armslist had designed its website to allow illegal sales of firearms, it was a creator of content rather than a mere intermediary.[220] On appeal, the Wisconsin Supreme Court held that Daniel's claims depended on treating Armslist "as a publisher or speaker of third-party content." The Court concluded that Daniel's causes of action inherently required treating Armslist as a publisher of third-party content. In other words, Daniel's claims rested on Armslist's liability from its role as a publisher by making the forum and third-party content available, knowledge that the site could be used for illegal purposes was, therefore, considered irrelevant.[221] That Court stated that Daniel's argument failed partially because it relied on a nonexistent "good faith" requirement under Section 230(c)(1).[222] Ultimately, the Supreme Court of Wisconsin agreed with the Circuit Court's determinations and reversed the Appellate decision.[223] The Supreme Court of the United States denied review on November 25, 2019.[224]

---

213 *Id.* at 468-69.
214 *Id.* at 469.
215 *Id.* at 472.
216 *Id.*
217 *Id.* at 474.
218 *Id.*
219 *Id.* at 461-462.
220 *Id.*
221 *Id.* at 475.
222 *Id*.
223 *Id.* at 463.
224 U.S. Supreme Court Docket No. 19-153.

C. The Duty of Online Service Providers

The Second and Third Restatements of Torts provide guidelines for determining whether a duty should be extended to landowners. A landowner whose conduct did not create the risk of harm generally does not have a duty of care, unless the court determines an affirmative duty exists by statute, prior conduct, special relationship, or undertaking.[225] However, pursuant to Restatement (Second) of Torts § 343: A landowner is subject to liability for a plaintiff's injuries or damages caused by conditions the landowner knew or should have discovered through the "exercise of reasonable care" that create an unreasonable risk of harm which the landowner failed to protect against.[226] In other words, in the online context, if the risk of harm from certain features on the website outweighs the burden of the provider in imposing available protective measures, the online service provider should be extended a duty to provide such, and be responsible for those decisions.

A duty to exercise reasonable care to protect users and others from dangerous conduct by third parties should not be limited to physical land operators, but should be extended to the virtual arena. Section 230 "was intended to promote the values of privacy, security and liberty alongside the values of open discourse."[227] The proposed duty would incentivize online service providers to implement features that protect individual's privacy, security, liberty, and free speech rights—thus adhering to Congress' goals in enacting Section 230.[228] An online service provider, like a land operator, is in the best position to protect against conditions that create an unreasonable risk of harm that they know about or could discover through the exercise of reasonable care. The decision of whether that duty has been breached turns on the foreseeability of the harm.[229]

An analysis of the online service providers' policies and features will help determine whether the provider knew, or should have known, that

---

225 *See* RESTATEMENT (THIRD) OF TORTS §§ 37-44 (AM. L. INST. 1995).

226 RESTATEMENT (SECOND) OF TORTS § 343 (AM. L. INST. 1965).

227 Citron & Franks, *supra* note 22 at 45, 51 (2020) (citing to Mary Anne Franks, *The Lawless Internet? Myths and Misconceptions About CDA Section 230,* HUFFINGTON POST, Feb. 17, 2014).

228 *See Fostering a Healthier Internet to Protect Consumers: Joint Hearing Before the Subcommittee on Communications and Technology and Subcommittee on Consumer Protection and Commerce*, 116th Cong. (2019) (statement of Danielle Keats Citron, Professor of Law, Boston University School of Law) ("Online behavioral advertising generates profits by 'turning users into products, their activity into assets,' and their platforms into 'weapons of mass manipulation.' Tech companies 'have few incentives to stop [online abuse], and in some cases are incentivized to ignore or aggravate [it].'"); Citron & Franks, *supra* note 22 at 45, 51.

229 *See* Martin v. Rite Aid of Pennsylvania, Inc., 2013 PA Super 299, 80 A.3d 813, 815 (2013).

harm was reasonably likely to occur. In the online context, numerous websites have enacted features that allow them to be notified by users for objectionable content.[230] However, many of these websites have failed to adequately equip themselves to address these numerous user notifications.[231] Note that, as discussed above, willful ignorance does not preclude liability and is not considered a valid excuse in law. There are several features that could be used to more adequately address dangerous content or conduct occurring on online platforms.[232]

Given the number of notifications that the defendant, Grindr, received from Herrick in *Herrick v. Grindr* and the dangerous nature of conduct occurring through the website in *Daniel v. Armslist*, the defendants in these cases knew, or had reason to know, that harm was foreseeable.[233] Moreover, the defendants were in the best position to protect against and remediate the conditions likely to result in harm. For example, in *Herrick v. Grindr*, Grindr failed to incorporate safety features like "common image recognition or duplicate-detection software" that could easily detect impersonating profiles like the ones created by Herrick's ex-boyfriend.[234] Once having been notified of the potential danger from the impersonating profiles, Grindr could have easily used one of the aforementioned programs to combat the dangerous condition.

Grindr should have had a duty to protect its users by discovering inherently dangerous conditions facilitated by its failure to use the aforementioned features. Grindr knew of the potential harm to Herrick by the profiles and could have implemented geofencing[235] to discover whether the account is associated with a particular individual's location, without significantly burdening itself. Instead, Grindr did nothing.[236]

---

230 *See generally* Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997); Jane Doe No. 1 v. Backpage.com LLC, 817 F.3d 12, 12 (1st Cir. 2016); Herrick v. Grindr, LLC, 306 F. Supp. 3d 579, 579 (S.D.N.Y. 2018); Daniel v, Armslist, LLC, 386 Wis. 2d 449, 449 (Wis. 2019).

231 *See* Shelley Ross Saxer, *"Am I My Brother's Keeper?": Requiring Landowner Disclosure of the Presence of Sex Offenders and Other Criminal Activity*, 80 NEB. L. REV. 522, 531 (2001) ("[F]oreseeability was based upon the magnitude of the risk and the fact that this concern had already been brought to the landlord's attention by other tenants in the building.").

232 *See* Herrick v. Grindr, LLC, 306 F. Supp. 3d at 590 (describing the features available to Grindr for addressing multiple profiles).

233 *See id.* at 593 ("Grindr ignored 'numerous complaints and requests for [it] to control its product and disable the [impersonating] accounts being used to destroy [Herrick's] life.'").

234 *Id.* at 585.

235 *Id.*

236 Brief for Petitioner at 10, Herrick v. Grindr, LLC, No. 19-192 (U.S. S. Ct. dismissed on Oct. 7, 2019) ("Grindr was the only one that could help, was on repeated notice, and was uniquely and exclusively qualified to do so. Yet, Grindr did nothing.").

Furthermore, in an effort to prevent the creation of duplicate profiles, Grindr could block the use of "spoofing, proxies, or virtual private networks (VPNs)."[237] In balancing Grindr's economic interests and Herrick's right to safety, it is evident that implementing at least one of the available features could have prevented or remediated the dangerous condition without overly burdening Grindr's business.

Similarly, in *Daniel v. Armslist*, Armslist knew or had reason to know that the feature allowing the anonymous purchase of firearms[238] could foreseeably result in harm. Anonymity in transactions involving firearms is inherently dangerous because sellers are unable to identify the purchaser's age or whether or not he or she is legally able to possess or purchase a firearm.[239] In deciding to implement this anonymity feature, Armslist chose to accept the potential risk of harm. Under the proposed duty, Armslist would not be required to change its operations if it finds its interests are better served by allowing such risky activity—meaning that it would be more cost effective to implement reasonable content moderation to avoid liability than not and risk being held liable. However, Armslist would be required to pay for the consequences facilitated by such a feature, or lack thereof. In applying the balancing approach for extending a duty, a court should have found that due to the available remedial or protective features, other than the removal of anonymity, the safety rights of Armslist's users and the general public outweigh Armslist's interests. This duty fits within the original purpose of Section 230 because it does not force Armslist to undertake any particular course of action, but rather, only prevents it from merely sitting back and watching dangerous conditions manifest harm without taking responsibility for the consequences its design choices facilitated. The proposed duty requires Armslist, and online service providers, to act in "good faith"—that which is reasonable in light of foreseeable harm—to discover and implement content moderation measures.[240]

---

237 *Id.*

238 *See* Daniel v. Armslist, LLC, 386 Wis. 2d 449, 460 (Wis. 2019).

239 *Internet Firearm Sales: ATF Enforcement Efforts and Outcomes of GAO Covert Testing* (Dec. 21, 2017) ("In 2016, the Center also issued a report about Internet firearm transactions. This and other ATF reports highlighted the following about Internet-facilitated firearm transactions: The relative anonymity of the Internet makes it an ideal means for prohibited individuals to obtain illegal firearms; The more anonymity employed by a firearms purchaser, the greater the likelihood that the transaction violates federal law; Firearm transactions that occur on the Dark Web are more likely to be completed in person or via the mail or common carrier, versus through a Federal Firearm Licensee.").

240 *See* Kim, *supra* note 20 at 1042 ("The intent underlying Section 230 immunity, at least as interpreted by courts, is to both permit Web site sponsors to monitor content and relieve them of the burden of doing so.").

Despite these useful features, it is highly probable that new loopholes or workarounds will continuously be created, thus making it difficult to always protect against all potentially dangerous content. However, a duty that requires online service providers to monitor these changes periodically and keep their protective measures relatively up to date, similar to that proposed in Citron and Wittes reasonable content moderation proposal, should be extended to online service providers—as is currently required of landowners under the theory of premises liability. Premises liability using the balancing test does not require landowners to *always* be up to date. Rather, it requires landowners to make concerted efforts to weigh their economic interests against individuals' rights.[241] This duty would force online service providers to choose user safety when the risk of harm outweighs the burden or cost of imposing such a measure.

Similarly, in premises liability, landowners are forced to implement protective or remedial measures when the risk of injury outweighs the cost of such an implementation.[242] Consider that if Grindr used a duplicate-detection software and geolocation feature to prohibit the creation of multiple profiles, imposters could have moved to the use of a virtual private network. In exercising reasonable care, Grindr would have discovered that features allowing it to search IP and MAC address search, as well as block the use of spoofing, proxies, and virtual private networks (VPNs), would have allowed Grindr to prohibit the creation of new impersonating accounts and locate the imposter.[243] Grindr would have a duty to decide which safety measures are necessary and would be responsible for those decisions.

Physical businesses that create conditions that make criminal activity more likely to occur have been held liable for such conduct.[244] For example, a hotel that has no night security and minimal lighting in the parking lot may be held liable for the criminal activity that takes place on the premises. Such conditions facilitate criminal activity, or at a minimum, make it easier or more likely for it to occur than if security measures had been implemented. Similarly, certain features on a website created by the online service providers facilitate criminal conduct. In *Daniel v. Armslist*, several features available on Armslist's websites, such as anonymity and the ability for unlicensed sellers, who do not require background checks,

---

241 Clarkson, *supra* note 112 at 629.

242 *See id.* at 628.

243 *Id.*

244 *Landlord's Liability for Failure to Protect Tenant from Criminal Acts of Third Person*, 43 A.L.R.5TH 207 (1996) (referring to § 4[b] Duty to Protect Against Reasonably Foreseeable Criminal Acts of Third Parties—Where Based on Physical Defect of Premises).

to sell dangerous weapons to nearly anyone[245] - facilitated or made criminal conduct more likely to occur.[246], Thus, these features provided a simple means for those with restricted access to firearms to obtain them.

The question for determining whether a duty should be extended in the online context is whether online service providers can continue to operate their businesses in a safer manner with different features.[247] Could Grindr have continued to operate successfully if it blocked the use of VPNs and used common-image recognition or duplicate-detection software? Could Armslist have continued its operation if it removed the anonymity feature or required purchasers from private sellers to reveal their identity? The answer would likely be yes—there were available measures that Grindr and Armslist could have taken that would not have severely burdened their operations. Nonetheless, they chose to operate their business in the manner described above and as such should be responsible for the consequences.

In summary, under traditional premises liability analysis, a landowner may be found liable for a dangerous condition present on his or her property, if he or she knew or should have known of the condition and failed to implement reasonable measures to protect against or remediate it before it caused an injury.[248] Dangerous design features in the online context fit within the premises liability framework.[249] If a website feature creates the risk of harm, and the operator knows or should know of this risk, and fails to exercise "good faith" moderation practices before an injury occurs, the website operator should be found liable, not be extended immunity.

Due to the newness and continuous expansion of the internet, new measures and loopholes around such will continuously present themselves. Nevertheless, online service providers should have a duty to exercise reasonable care in protecting against dangerous third-party conduct that creates an unreasonable risk of harm through the use of their services. The duty proposed does not require online service providers to provide a perfectly safe internet space, but requires operators to balance the interests in deciding what reasonable features, measures, or policies to

---

245 Daniel v. Armslist, LLC, 386 Wis. 2d 449, 449 (Wis. 2019).

246 RESTATEMENT (SECOND) OF TORTS § 344. cmt. f. (AM. L. INST. 1995).

247 Scott W. Weatherford, Comment, *The Ad Hoc Duty: A Landowner's Duty to Protect After Del Lago Partners v. Smith*, 63 BAYLOR L. REV. 565, 568 (2011) (quoting Gen. Electric Co. v. Moritz, 257 S.W.3d 211, 216-18 (Tex. 2008)).

248 *See* Steven D. Winegar, Comment, *Reapportioning the Burden of Uncertainty: Storekeeper Liability in the Self-Service Slip-and-Fall Case*, 41 UCLA L. REV. 861, 866 (1994).

249 *See* Citron & Wittes, *supra* note 14 at 468 ("Designing a site to enable defamation or sex trafficking could result in liability in the absence of a finding that a site was being sued for publishing or speaking.").

implement to prevent foreseeable harm. The duty proposed is consistent with Section 230: A duty to exercise "good faith" – that is, reasonable and directed at foreseeable harm- moderation practices. This duty requires online service providers to act in "good faith" rather than reward those who fail to moderate content *at all*, even when it is likely to cause harm.

D. Causation

For the causation element to be satisfied, a plaintiff must show but-for causation and proximate causation.[250] A defendant's conduct is the but-for cause of a plaintiff's injuries or damages when the defendant's conduct—in the case of premises liability, the defendant's failure to exercise reasonable care in protecting and remedying a dangerous condition—was a substantial factor in bringing about plaintiff's harm and the harm would not have resulted but-for the defendant's conduct.[251] Proximate cause turns on the foreseeability of the harm—whether the consequences were the foreseeable result of the defendant's conduct, or lack thereof.[252]

To determine whether the defendant's features are the but-for cause, the court should ask whether the criminal activity or intentional tort would have been carried out through the means used had other available and safer features been implemented. In the context of criminal attacks, the question becomes difficult to answer because it is hard to pinpoint exactly what measures would have prevented or stopped a criminal attack.[253] In the online context, where individuals are able to remain anonymous and hidden behind the screen of an electronic device, the only thing likely to prevent criminal or intentionally tortious content online are those features implemented by the platforms themselves. This is evident through the use of "Terms & Conditions" implemented by online service providers. For example, in *Grindr*, Herrick's ex-boyfriend may have been deterred from making multiple impersonating profiles if Grindr had implemented and enforced policies that prohibited such.

The features on Grindr's application and Armslist's website were substantial causal factors resulting in the plaintiffs' injury. However, being a substantial causal factor is not sufficient to qualify as being the but-for cause, the other possible causal factors must be insignificant or removed from the event.[254] Without the use of Grindr's application, Herrick's ex-boyfriend would not have been able to send numerous individuals in

---

250 Holmes v. Campbell Properties, Inc., 47 So.3d 721, 724 (Miss. Ct. App. 2010).

251 *Id.* at 724-25.

252 *Id.* at 724.

253 *See* Mark Geistfeld, *Tort Law and Criminal Behavior (Guns)*, 43 ARIZ. L. REV. 311, 316-17 (2001).

254 *See* RESTATEMENT (SECOND) OF TORTS § 431 (AM. L. INST. 1995) (comment on what constitutes legal cause).

search of rough sexual encounters to Herrick's workplace and home. On this point it is important to note that Herrick's ex-boyfriend attempted to commit the same scheme on other applications that once having been notified, rectified the dangerous condition in a timely manner.[255] Therefore, but-for Grindr's negligence—or failure to implement good faith content moderation practices that would allow it to operate in a reasonably safe condition in light of foreseeable harm, like the other applications—users would not have been sent to Herrick's residence causing him to be harassed and harmed. In *Daniel v. Armslist*, Houghton would have found it more difficult to obtain a firearm given the restraining order filed against him. However, because of the design features created by Armslist.com, Houghton was able to easily obtain the firearm without a trace and commit the attack in a matter of days. Armslist's features were the reason why Houghton was able to go onto the site and easily obtain a firearm. Although it is possible that Houghton could have done this offline, he would not have been able to maintain anonymity and he would have had to engage in a longer and more tedious search, which wouldn't have allowed him to get a firearm within just two days. Therefore, Armslist's negligent design features were the but-for cause of Daniel's injuries because the other potential causal factors are insignificant.

The inquiry for determining proximate cause is one of foreseeability.[256] Foreseeability is involved in both determining whether a duty should be extended and whether the defendant's conduct was the proximate cause. However, courts analyze foreseeability for duty and foreseeability for proximate causation separately—they are two distinct and independent elements.[257] The foreseeability analysis for determining whether there is a duty is a broader more general inquiry compared to the fact-specific analysis required for the determination of proximate cause.[258] A court examining duty does not look specifically to the conduct or characteristics of the defendant, but rather on the general event.[259] On the other hand, the causation inquiry is fact specific—whether the specific behavior by that specific defendant could foreseeably lead to injury.[260] Thus, courts decide whether proximate cause exists on a case-by-case basis.

---

255 Petition for a Writ of Certiorari at 5, Herrick v. Grindr, LLC, No. 19-192 (2019).

256 *See* Rogers v. Martin, 63 N.E.3d 316, 325 (Ind. 2016).

257 Michael Campbell, Comment, *Ballpark Beatdowns: A New Framework to Protect Fans*, 22 S. CAL. INTERDISC. L. J. 109, 124 (2012).

258 Goldsberry v. Grubbs, 672 N.E.2d 475, 479 (Ind. Ct. App. 1996).

259 *See* Cody J. Jacobs, *Guns in the Private Square*, 2020 U. ILL. L. REV. 1097, 1113 (2020).

260 *Id.*

In the online context, courts should consider several factors in their proximate cause analysis.[261] In premises liability, courts take into account factors that could have prevented the injury—for example, the policies in place at the premises and the characteristics of the perpetrator of the crime or intentional tort. Similarly, these factors should be used in the proximate cause analysis in the online context. In applying the theory of premises liability to the online context, courts should consider whether the plaintiff's injuries or damages from the particular crime or tort would have been prevented had the online service provider implemented other available protective or remedial features or more stringent policies.

Courts should account for several factors in determining whether proximate causation exists. In the cases of *Grindr* and *Armslist*, courts should consider whether the defendants were notified, the number of users, and available preventative features, just to name a few. For example, courts should consider the fact that Grindr's competitor was able to combat the fraudulent scheme while Grindr wasn't, while accounting for the fact that Grindr was a larger platform.[262] Additionally, in the case of *Armslist*, courts should consider the inherently dangerous content allowed by the website to determine the foreseeability of harm. The online service providers in *Grindr* and *Armslist* are distinct and thus, the factors to be analyzed differ and would be weighed differently. Accordingly, the determination is fact specific.

In both *Herrick v. Grindr* and *Daniel v. Armslist*, the defendants were notified numerous times of the dangerous condition and chose to ignore the risk. Once having been notified, they should have had a duty to exercise reasonable care in protecting against the potential harm. Under the theory of premises liability, a store that is notified of a wet floor has a duty to address the risk to protect against the potential harm. In that case, the store could clean up the mess or place a sign to warn customers. If the store chooses to ignore the dangerous condition altogether, the store's omission could be found to be the proximate cause of a plaintiff's injury. Similarly, online service providers that ignore the dangerous conditions on the websites they created and that are under their operation and control are the proximate cause of the harm from those conditions. The fact that the spill, in the case of a physical premises, or attacks, in the cases of *Grindr*

---

[261] *See* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 Berkeley Tech. L. J. 1553, 1585 (2005) ("Courts should examine factors such as: (1) whether there have been prior similar cybercrimes; (2) the cost of increased internet security measures; and (3) the degree to which intermediaries can reduce the radius of the cybercrime problem.").

[262] Brief for Petitioner at 5, Herrick v. Grindr LLC, No. 19-192 (U.S. S. Ct. dismissed on Oct. 7, 2019).

and *Armslist*, were ultimately completed by third parties does not break the chain of causation.

CONCLUSION

A laudable goal of Section 230 is to encourage online service providers to make "good faith" effort to moderate potentially dangerous content present on their platforms. The history of Section 230 illustrates how courts have made decisions that directly contradict this mission to incentivize online intermediaries. The theory of premises liability, based on traditional tort principles, should be applied to the online context. Extending a duty of care to online service providers, not being treated as publishers, will incentivize them to implement safety measures and to internalize the costs of their design decisions. Moreover, in looking at how causation has been found in premises liability cases, courts can apply the same concepts to online liability cases. Applying the theory of premises liability to the online context would make it possible to hold online service providers responsible for failing to moderate content it knows can foreseeably result in harm, thus encouraging them to make reasonable efforts to protect against such conditions while also adhering to the concept of immunity for acting solely as publishers. This is illustrated by the application of premises liability to the recent cases of *Herrick v. Grindr* and *Daniel v. Armslist*. Only when online service providers are treated like classic publishers can they be provided with the shield of Section 230 and only when "good faith" efforts are made to protect against foreseeable harm should online service providers escape liability.