The Communication Decency Act Gone Wild: A Case for Renewing the Presumption Against Preemption

Ryan J.P. Dyer[*]

"The Communications Decency Act was not meant to create a lawless no-man's-land on the Internet."[1]

I. INTRODUCTION

Few things in history have expanded the reach of human enterprise like the Internet. Since its inception, the Internet has disseminated the most vital commodity known to man—information. But not all information is societally desirable. In fact, much of what the Internet serves to disseminate is demonstrably criminal. Nevertheless, in the effort to unbind the "vibrant and competitive free market" of ideas on the Internet, Congress enacted section 230 of the Communications Decency Act (CDA).[2] In essence, section 230 of the CDA grants immunity to "interactive computer service providers"[3] (ICSPs) from liability for information provided by a third party.[4] Courts have broadly applied section 230's grant of immunity to bar plaintiffs seeking to hold ICSPs liable for third-

[*] J.D. Candidate, Seattle University School of Law, 2014; B.S., Economics, Central Washington University, 2009. I would like to thank the *Seattle University Law Review*, including Kiera Miller, Nick Franzen, and Alex Caggiano, whose diligent efforts made this Comment publishable. I would also like to thank my parents, Tom and Doreen Dyer, and my wife, Maggie Dyer, for their unstinting support and encouragement over the last two years.

1. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1164 (9th Cir. 2008) (writing for the majority, Chief Judge Kozinski noted that "[t]he Internet is no longer a fragile new means of communications that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant—perhaps the preeminent—means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of immunity provided by Congress and . . . comply with laws of general applicability." *Id.* at n.15).

2. The Communications Decency Act, Protection for Private Blocking and Screening of Offensive Material, 47 U.S.C. § 230 (1998) [hereinafter section 230] (codified as amended in scattered sections of 47 U.S.C.).

3. For all intents and purposes—"websites."

4. 47 U.S.C. § 230(c) (1996).

party content posted to their websites.[5] However, as the Internet permeates deeper into modern society, an increasing amount of criminal activity is finding refuge behind outdated and obtuse constructions of section 230's immunity provisions.[6] Consequently, state and local governments are faced with a diminishing capacity to properly confront the widening array of criminal activity perpetrated via the Internet.[7]

Section 230 has garnered significant attention since its enactment, and many commentators have noted the sweeping impunity it has bestowed upon websites that host third-party content.[8] The initial scope of immunity provided by courts applying section 230, as well as the practical consequences of its continued construction, is well documented.[9] This Comment strives to explain why courts applying section 230 today—over fifteen years after its enactment and in the face of flagrantly criminal complicity on the part of websites—continue to accept the preemptive scope established by early courts. More specifically, this Comment suggests that, in certain contexts, courts applying section 230 immunity should reexamine the preemptive effect Congress intended section 230 to have on traditional state police powers.[10] Doing so would not only reveal the unwarranted scope of activities currently deemed immune under section 230, but would also redeem the ability of state and local authorities to combat the increasing amount of criminal activity on the Internet.[11]

Part II of this Comment outlines the legislative history and intent of section 230, as well as the evolution of judicial construction and application of the statute's immunity-granting provision. Part III discusses how early courts' over-expansive interpretation of section 230, coupled with the current proliferation of cybercrime, is increasingly paralyzing states' efforts to combat crime perpetrated via the Internet. Part IV identifies the locus of continued misconstruction by courts applying section 230 as the failure to reevaluate Congress's preemptive intent in light of the changing dynamic on the Internet. Part V analyzes the several judicial and legislative solutions that could alleviate the strain that section 230 immunity

---

5. *See infra* Part II.B.

6. *See infra* Part III.A.

7. *See infra* Part III.B–C.

8. *See* 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, 410–12 (2010).

9. *See infra* Part II–III.

10. *See infra* Part IV.

11. *See infra* Part IV. *See generally* INTERNET CRIME COMPLAINT CTR., FED. BUREAU OF INVESTIGATIONS, 2012 INTERNET CRIME REPORT (2013), *available at* http://www.ic3.gov/media/annualreport/2012 _IC3Report.pdf.

puts on state and local efforts to deal with criminal activity perpetrated via the Internet. Finally, Part VI offers a brief conclusion.

II. THE CONCEPTION & APPLICATION OF SECTION 230

Section 230's inclusion as part of the CDA represented Congress's desire to remove the disincentives for online intermediaries to police activity on their websites. The new provision arrived with a splash as early courts gave section 230's scope of immunity expansive effect.[12] Originally, the provision was intended to encourage the *removal* of offensive content; instead, it has developed into a broad grant of immunity for websites that host offensive and criminal content.

A. A Brief History

The Communications Decency Act of 1996 was enacted at the height of a national struggle between explosive growth in the telecommunications industry[13] and resurgent social conservatism.[14] Senator James Exon from Nebraska spearheaded the legislation, intending to combat the danger posed to the youth of America[15] by "barbarian pornographers."[16] Several CDA provisions were widely scrutinized for their questionable constitutionality.[17] Eventually, in *Reno v. ACLU*, the Supreme Court struck down portions of the Act that criminalized the transmission of indecent material accessible to minors.[18] Yet most of the Act still remained intact, including section 230.

Section 230, titled "Protection for Private Blocking and Screening of Offensive Material," was created "to promote the continued development of the Internet."[19] At the time of the CDA's creation, Congress

12. *See infra* Part II.B.

13. WALTER SAPRONOV & WILLIAM H. READ, TELECOMMUNICATIONS: LAW, REGULATION, AND POLICY xi (1998).

14. For additional background on the social conservative movement in the mid-1990s, see DONALD T. CRITCHLOW, THE CONSERVATIVE ASCENDANCY: HOW THE GOP RIGHT MADE POLITICAL HISTORY (2007).

15. For an extensive discussion regarding the legislative history of the CDA, see Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51 (1996).

16. 141 CONG. REC. S8339 (daily ed. June 14, 1995) (statement of Senator Exon) (quoting Brock N. Meeks).

17. *See* Cannon, *supra* note 15, at 65–72 (discussing the popular opposition to introduction of the CDA amongst member of the Senate and House of Representatives).

18. Reno v. ACLU, 521 U.S. 844, 885 (1997) (invalidating provisions of section 223(a) and (d) except as applied to child pornography).

19. 47 U.S.C. § 230(b) (1996).

doubted certain CDA provisions would survive constitutional scrutiny[20] and thus enacted section 230 as a "complementary backstop" to the Act's more dubious provisions.[21] Congress was also motivated to override a recent decision of a New York trial court in *Stratton Oakmont, Inc. v. Prodigy Services*.[22]

In *Stratton Oakmont*, an ICSP was held liable for a third party's libelous statements posted on its computer bulletin boards.[23] The ICSP exercised *some* editorial control over the content posted on its interactive user bulletin boards and touted itself as a family-oriented computer network.[24] The court held that because the ICSP had exercised some editorial control over its bulletin boards, it could be held liable under a publisher theory of liability just like a brick-and-mortar newspaper or magazine.[25]

Concerned that the decision in *Stratton Oakmont* would serve as a disincentive for ICSPs to exercise *any* editorial control over third-party content posted to their sites lest they incur full publisher liability, Congress responded by including section 230 in the CDA.[26] Specifically, Representatives Christopher Cox and Ron Wyden proposed an amendment to the draft CDA (the Cox–Wyden Proposal).[27] The Cox–Wyden Proposal sought to address the dilemma *Stratton Oakmont* created by removing traditional forms of publisher liability for ICSPs who acted in good faith to restrict access to offensive content.[28] However, unlike the provisions Senator Exon advocated,[29] the Cox–Wyden Proposal did not affirmatively *require* ICSPs to make good faith efforts to qualify for im-

20. *See* 141 CONG. REC. S8331 (daily ed. June 14, 1995) (statement of Sen. Leahy).

21. *See* David Lukmire, Note, *Can the Courts Tame the Communications Decency Act?: The Reverberations of* Zeran v. America Online, 66 N.Y.U. ANN. SURV. AM. L. 371, 375 (2010).

22. Stratton Oakmont v. Prodigy Servs., No. 31063/94, 1995 N.Y. Misc. LEXIS 229, at *3–4 (N.Y. Sup. Ct. May 25, 1995).

23. *Id.* at *17–18.

24. *Id.* at *2.

25. *Id.* at *10–11.

26. The congressional approval of such action can be seen in 47 U.S.C. § 230(b)(4); *see also* H.R. Rep. No. 104-458, at 194 (1996), *reprinted in* 1996 U.S.C.C.A.N. 10 ("One of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material.").

27. 141 CONG. REC. 22044–45 (amendment offered by Rep. Cox).

28. *Id.*

29. *See* sources cited *supra* note 16 and accompanying text.

munity.[30] Nevertheless, both the Exon and Cox–Wyden Proposals were enacted as part of the CDA.

The immunity-granting provision of section 230 provides as follows:

> (c) Protection for "good samaritan" blocking and screening of offensive material
>
> (1) Treatment of publisher or speaker
>
> 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.[31]

Section 230 expansively defines an "interactive computer service" to include all online service providers and websites;[32] an "information content provider" is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[33] Congress attempted to limit the scope of immunity by stating that section 230 would have no effect on federal criminal statutes, intellectual property law, communications privacy law, or "any State law that is consistent with this section."[34] However, subsection (c) has unintentionally become the most impactful language within the entire CDA, controlling virtually every cause of action against ICSPs.[35]

B. Judicial Treatment

Generally, courts broadly interpret section 230 and the immunity it provides ICSPs. As discussed below, early courts benefited from factual

---

30. *Id.* In this way, the Cox–Wyden Proposal differed from the provisions Senator Exon advocated, which required good faith efforts in to qualify for immunity and were subsequently struck down by the court in *Reno v. ACLU*. 47 U.S.C. § 223(f)(1) (1996).

31. 47 U.S.C. § 230(c)(1) (1996).

32. Specifically, an "interactive computer service" is "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educations institutions." 47 U.S.C. § 230(f)(2) (1996). Courts have construed interactive computer service broadly to include websites. Batzel v. Smith, 333 F.3d 1018, 1030 n.16 (9th Cir. 2003).

33. 47 U.S.C. § 230(f)(3) (1996).

34. *Id.* § 230(e)(3).

35. For an extensive compilation of cases and their outcomes involving the widespread usage of section 230, see Ken S. Myers, *Wikimunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. J.L. & TECH. 163 (2006); *see also* Claudia G Catalano, Annotation, *Validity, Construction, and Applications of Immunity Provisions of Communications Decency Act, 47 U.S.C.A. § 230*, 52 A.L.R. FED.2d 37 (2011).

circumstances mirroring the context in which section 230(c) was meant to apply. However, the first courts to interpret and apply section 230 went "further than was necessary to effectuate the congressional goals" of the statute's immunity-granting provision.[36] Although unapparent at first, this over-expansive reading of section 230(c) laid the groundwork for broad applications of immunity by future courts in contexts blatantly incommensurate with the statutes intended scope and effect.

The first major case interpreting section 230 was the Fourth Circuit's decision in *Zeran v. America Online, Inc*.[37] Plaintiff Zeran was the subject of a hoax in which an unidentified person advertised t-shirts displaying offensive slogans related to the recent Oklahoma City bombing.[38] The posted advertisement appeared on America Online's (AOL) public message boards and listed Zeran's phone number, urging viewers to contact Zeran for more information.[39] Zeran was quickly inundated with threatening phone calls from viewers of the ad, and the next day he called AOL to complain.[40] AOL agreed to remove the ad but did not issue a retraction, and shortly after, similar ads continued to appear.[41] Zeran filed suit claiming that once AOL received notice of the fallacious postings, it had a duty to remove the postings, issue a retraction, and prevent a reoccurrence.[42]

In an attempt to give far-reaching effect to Congress's intent to overrule *Stratton Oakmont*, the Fourth Circuit broadly interpreted section 230's scope of immunity afforded ICSPs.[43] Specifically, the court interpreted the section 230(c) safe harbor provisions to confer immunity to ICSPs for a broad range of claims including "tort-based lawsuits" and "tort liability."[44] The Fourth Circuit's interpretation represented a far-reaching application of section 230(c), which previously had been thought to target mainly defamation-based claims.[45] Furthermore, the

36. *See* Lukmire, *supra* note 21, at 385.
37. Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).
38. *Id.* at 329.
39. *Id.*
40. *Id*.
41. *Id*.
42. *Id.* at 330.
43. *Id.* at 328.
44. *Id.* at 330.
45. *See* Lukmire, *supra* note 21, at 395–99 (2010). Lukmire contends:
Properly read, *Zeran*, at its most expansive, ought to have stood for the proposition that section 230 conferred immunity on Internet entities only insofar as third-party content caused 'defamation-type' harms. The court's reliance on doctrine exclusive to defamation law to establish that 'distributor liability is a subset of publisher liability' contradicts the notion that sections 230's safe harbor extends to any legal malfeasance perpetrated by

court repeatedly stated that free speech concerns had been a major factor motivating Congress to enact the section 230(c) safe harbor provisions[46]—a proposition not necessarily supported by the provision's text or history.[47] Nevertheless, *Zeran* established the precedent for broad grants of immunity under section 230(c), a standard currently followed by a majority of both federal and state courts.[48]

For more than a decade, the broad immunity afforded by the holding in *Zeran* stood as an insurmountable barrier for plaintiffs seeking to impose liability on ICSPs. For example, in *Batzel v. Smith*, the Ninth Circuit faced the issue of whether an operator of an Internet site maintaining an electronic newsletter was liable for selecting and publishing an allegedly defamatory e-mail.[49] The court instructed that "the exclusion of 'publisher' liability necessarily precludes liability for exercising the usual prerogative of publishers to choose among proffered material and to edit the material published while retaining its basic form and message."[50] While a publisher could encounter liability for substantial alterations, the *Batzel* court's holding turned on the fact that the operator made no material contribution to the e-mail at issue during the editing process and therefore was not responsible for the e-mail's defamatory content.[51]

Similarly, in *Doe v. MySpace, Inc.*, a Texas district court declined to hold MySpace liable for failing to implement safety measures to protect minors from online sexual predators.[52] The plaintiff attempted to rely on state common law tort principles and alleged liability on the theory that because MySpace "knew sexual predators were using the service to communicate with minors . . . it was foreseeable that minors such as Julie

---

a third party.

Id. at 395–96 (citations omitted).

46. *Zeran*, 129 F.3d at 330–31, 333–35.

47. *See* Lukmire, *supra* note 21, at 385, 389.

48. *See, e.g.*, Barrett v. Rosenthal, 146 P.3d 510, 514 (Cal. 2006) (describing *Zeran* as the leading case interpreting section 230 immunity); *see also id.* at 518 n.9 (listing state and federal cases following *Zeran*'s interpretation of section 230 immunity). Specifically, courts have relied on *Zeran* to establish three elements required for section 230 immunity: "(1) the defendant must be a provider or user of an 'interactive computer service'; (2) the asserted claims must treat the defendant as a publisher or speaker of information; and (3) the challenged communication must be 'information provided by another information content provider.'" Batzel v. Smith, 333 F.3d 1018, 1037 (9th Cir. 2003) (citations omitted).

49. *Batzel*, 333 F.3d at 1031.

50. *Id.*

51. *Id.*

52. Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 848 (W.D. Tex. 2007). The plaintiff, a thirteen-year-old girl, had misrepresented her age when creating an online profile on MySpace's social networking site and was subsequently contacted by an adult man who allegedly perpetrated a sexual assault on her. *Id.* at 846.

Doe could be injured by the criminal acts of adult MySpace users."[53] The court disagreed and, relying heavily on *Zeran*, held that MySpace was merely an intermediary "provid[ing] its services to users for free" and thus fell squarely within the safe harbor provisions of section 230(c).[54]

In contrast, the first case seriously limiting the application of section 230 immunity was the Ninth Circuit's en banc decision in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC* (*Roommates*).[55] The Housing Council sued Roommates.com for matching individuals based on their answers to mandatory online questions concerning criteria banned by the federal Fair Housing Act[56] and California housing discrimination laws.[57] Despite Roommates.com's undisputed status as an "interactive service provider" within the meaning of section 230, the plaintiff alleged the site was more than a mere publisher of information provided by its users.[58] Instead, Roommates.com was acting as an "information content provider" because the site created, posted, required completion of, and disseminated the results of unlawful questionnaires.[59] In a divided opinion,[60] the court agreed that Roommates.com's activities were sufficient to make it "'responsible . . . in part' for creating or developing" content, and thus, Roommates.com failed to fulfill the third element of section 230(c) and was not entitled to immunity.[61]

The *Roommates* decision received mixed reviews from legal scholars and Internet-industry observers.[62] Many commentators felt that the *Roommates* court had created a "slippery slope" by assigning such an extensive definition to the term "development."[63] Others regarded the move as a necessary limitation to the provisions of section 230, which

53. *Id.* at 851.

54. *Id.* at 850.

55. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).

56. *See* Fair Housing Act, 42 U.S.C. § 3604 (1988); *see also* CAL. GOV'T CODE § 12955 (2012).

57. *Roommates.com*, 521 F.3d at 1162.

58. *Id.* at 1164–65.

59. *Id.*

60. The court split 8–3 with Chief Judge Kozinski writing for the majority and Judge McKeown concurring in part and dissenting in part. *Id.* at 1160, 1176.

61. *Id.* at 1165–69. The third element requires that the challenged communication must be "information provided by another information content provider" and not by the ICSP itself. *Id.* at 1162 (quoting 47 U.S.C. § 230(f)(3) (1996)).

62. *See* Eric Weslander, *Murky "Development": How the Ninth Circuit Exposed Ambiguity Within the Communications Decency Act, and Why Internet Publishers Should Worry*, 48 WASHBURN L.J. 267, 290–94 (2008).

63. *Id.* at 293–95.

had fostered an unchecked environment of "internet exceptionalism."[64] What was clear was that the holding in *Roommates* opened the door to new theories of exclusions to section 230 immunity.[65]

A particular piece of language from the *Roommates* decision provided the basis for arguably the narrowest application of section 230's safe harbor provisions. In defining the term "develop," the *Roommates* court noted that "a website helps to develop unlawful content, and thus falls within the exceptions to section 230, if it *contributes materially to the alleged illegality of the conduct*."[66] A discrepancy immediately emerged regarding the application of the "underlying illegality" test: is express "solicitation" on the part of the ICSP required, or is mere "inducement" sufficient to trigger liability?[67] To date, most cases have required that the defendant explicitly solicit illegal content.[68] However, in *NPS LLC v. StubHub, Inc.* (*StubHub*),[69] a Massachusetts trial court expansively applied *Roommates*'s articulation of develop and denied immunity to an ICSP for merely inducing the creation of illegal content.[70] The inducement standard articulated in *StubHub* apparently does not require an actual request and can occur even when third parties retain unfettered discretion over the content.[71] Although the exact contours of the theory are unclear, liability under an inducement standard is based on an indistinct determination that the defendant's actions influenced a third party's decision to post illegal content.[72]

---

64. *See* Lukmire, *supra* note 21, at 398–99; *but see* Varty Defterderian, Fair Housing Council v. Roommates.com*: A New Path for Section 230 Immunity*, 24 BERKELEY TECH. L.J. 563, 564 (2009).

65. *See* Weslander, *supra* note 62, at 293–97; Jeffrey R. Doty, *Inducement or Solicitation? Competing Interpretations of the "Underlying Illegality" Test in the Wake of* Roommates.com, 6 WASH J. L. TECH. & ARTS 125, 129–32 (2010).

66. *Roommates.com*, 521 F.3d at 1168 (emphasis added).

67. For an extensive discussion of the "underlying illegality" test, see Doty, *supra* note 65, at 126; *see also* Zac Locke, *Asking for It: A* Grokster*-Based Approach to Internet Sites That Distribute Offensive Content*, 18 SETON HALL J. SPORTS & ENT. L. 151 (2008).

68. *See, e.g.*, Fed. Trade Comm'n v. Accusearch Inc., 570 F.3d 1187 (10th Cir. 2009); Best Western Int'l, Inc. v. Furber, No. CV-06-1537-PHX-DGC, 2008 WL 4182827 (D. Ariz. 2008); Woodhull v. Meinel, 202 P.3d 126 (N.M. Ct. App. 2008).

69. NPS LLC v. StubHub, Inc., No. 06-4874-BLS1, 2009 WL 995483 (Mass. Dist. Ct. Jan. 26, 2009). In *NPS v. StubHub*, the New England Patriots brought suit against StubHub alleging tortious interference by allowing season ticket holders to unlawfully sell their tickets. *Id.* at *4. StubHub operated a website that allowed users to buy and sell tickets to sporting, concert, theater, and other live entertainment events. *Id.* at *2. StubHub did not buy or sell the tickets directly but it did profit from the transactions and facilitated these ticket sales in a number of ways. StubHub even allowed sellers to "mask" the ticket location by listing a seat up to five rows away, making it impossible for the Patriots to determine which ticket holders were selling their tickets. *Id.* at *3.

70. *See id.*

71. *Id.* at *12–13.

72. *Id.*

The first courts to apply section 230 inferred an exaggerated statutory meaning and intent to the statute's immunity-granting provision, rarely reexamining the basis of those findings. Several early courts have crafted various frameworks to exempt section 230 immunity; however, they have done so through a more limited analytical framework, focusing on section 230's mechanics and definitions.[73] Courts have yet to delve deeper into an analysis of the preemptive intent Congress envisioned for section 230. This is especially troubling given the increasing frequency that section 230 immunity is invoked in non-defamation contexts and the preemptive effect that necessarily follows other state civil and criminal laws.

III. SECTION 230'S INCREASING IMPACT ON LAW ENFORCEMENT

The ever-increasing migration of human activity to computer technology, specifically the Internet, has encapsulated nearly every aspect of society. Unsurprisingly, this shift includes an increasing amount of criminal activity, which has been transformed into a new and more diffuse form—cybercrime.[74] Traditional modes of law enforcement are not well adapted to combat cybercrime because it differs from traditional crime in several fundamental ways. Nevertheless, section 230's over-application into non-publisher forms of liability—such as distributor liability—has quickly invaded numerous forms of state civil and criminal liability that would normally serve as effective tools for combating cybercrime. The effect is an utter preemption of state laws as applied to ICSPs engaged in criminal activity, rendering states helpless to enforce their historic police powers to combat the proliferation of cybercrime.

A. The Proliferation of Cybercrime

Cybercrime essentially encompasses three distinct categories. In the first category, the actual computer and associated information technology is the target of the offense; the perpetrator often employs hacking, virus dissemination, or the interruption of computer services.[75] The second category entails a traditional crime where the computer and Internet

---

73. *See generally* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008); *StubHub*, 2009 WL 995483; Jones v. Dirty World Entertainment Recordings, LLC, 840 F. Supp. 2d 1008 (E.D. Ky. 2012).

74. "Cybercrime" essentially denotes the use of computer technology to achieve an unlawful purpose. *See generally* Susan W. Brenner, *Is There Such a Thing As "Virtual Crime"?*, 4 CAL. CRIM. L. REV. 1 (2001).

75. *See* Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465, 468–69 (1997).

merely play an incidental role; for example, a ransom note sent by kidnappers via e-mail.[76] The third and final category also consists of traditional crimes, but the computer and Internet play an instrumental role in carrying out the offense.[77] Common examples of this category include identity theft, fraud, fencing stolen property, and commercial sex advertising.[78] Traditional modes of law enforcement cannot effectively combat most forms of cybercrime because of the inherent differences between cybercrime and the traditional crimes law enforcement have evolved to combat.[79] Specifically, cybercrime differs from traditional crime because it is physically diffuse and frequently occurs on a much broader scale.[80]

Given the inherent challenges of combatting cybercrime, it is simply unfeasible for law enforcement to address every instance.[81] One viable alternative is for law enforcement to focus on the various technological intermediaries necessary to conduct Internet activity in general.[82] Such intermediaries generally fall into three categories.[83]

The first category includes intermediaries that provide the network and infrastructure to facilitate the physical transportation of data across the Internet.[84] Intermediaries in this category typically operate solely as passive conduits transmitting the data between users and other intermediaries.[85] Common examples of this first category include cable Internet providers, satellite providers, or wireless carriers.[86]

---

76. *See generally id.*

77. *See generally* Brenner, *supra* note 74.

78. *Id*.

79. *See* Susan Brenner, *Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?*, 30 RUTGERS COMPUTER & TECH. L.J. 1, 25 (2004). Professor Brenner identifies four primary components of cybercrime that differ inherently from most traditional criminal activity. First, cybercrime does not require "any degree of physical proximity between victim and victimizer at the moment the 'crime' is committed." *Id*. at 25 (footnote omitted). Second, cybercrime is not confined to a definite scale because the internet "acts as a force multiplier that vastly increases the number of 'crimes' an individual can commit." *Id*. at 28 (footnote omitted). Third, "perpetrators of cybercrime are not restricted by the [physical] constraints that" otherwise govern perpetrators of traditional crimes. *Id*. at 30 (footnote omitted). Finally, the novel nature of cybercrime means that law enforcement "cannot identify patterns comparable to those that exist for real-world crime." *Id*. at 33 (footnote omitted).

80. For an extended discussion of the distinctions between cybercrime and traditional crime, see Brenner, *supra* note 74, at 25–40.

81. *Id*.

82. *See* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1585 (2005).

83. *See* Ardia, *supra* note 8, at 386.

84. *See* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 664 (2003).

85. *See* Ardia, *supra* note 8, at 386–87.

86. *See generally* Zittrain, *supra* note 84.

The second category of intermediary is comprised of content hosts that store, cache, or otherwise provide users with access to third party generated content.[87] Essentially, these conduit intermediaries either host the servers that store online content created by third parties or create the websites that allow users to access content, often assuming both functions.[88] Common examples include websites such as Yahoo, Facebook, and GoDaddy. The third and final category of intermediaries includes search engines and application service providers, which essentially provide tools for finding, indexing, filtering, and formatting content.[89] Common examples include Google, Bing, and various spam-filtering software.

The first and third types of intermediaries—those that serve as passive conduits and provide neutral search tools—are generally only passively monitored by law enforcement.[90] This is because both types of intermediaries typically only serve as passive mediums, which criminals misappropriate to unlawful ends, even though the vast majority of activity is perfectly legal.[91] Alternatively, the second form of intermediary—comprised of content hosts—can directly and affirmatively enhance the unlawful activities' effects.[92] This is most often true in situations where the website is largely devoted to hosting or providing a forum for the unlawful conduct in question. For example, a gossip website that encourages posting of frivolous information and rumors on its message boards materially contributes to any defamatory postings that result.[93] Or a ticket resale website that facilitates the resale of pre-purchased tickets materially enhances the violation of state anti-scalping laws.[94] Or even a classifieds website that hosts large quantities of commercial sex advertisements materially facilitates prostitution, human trafficking, and child exploitation.[95]

---

87. *See* Jack M. Balkin, *Media Access: A Question of Design*, 76 GEO. WASH. L. REV. 933, 936–37 (2008).

88. *See generally* Ardia, *supra* note 8.

89. *Id*. at 389.

90. *See* Brenner, *supra* note 74, at 55–65 (discussing the need for law enforcement to work cooperatively with the public to monitor websites for criminal activity).

91. *Id*.

92. *See generally* Rustad & Koenig, *supra* note 82.

93. *See* Jones v. Dirty World Entertainment Recordings, LLC, 840 F. Supp. 2d 1008, 1010 (E.D. Ky. 2012).

94. *See* NPS LLC v. StubHub, Inc., No. 06-4874-BLS1, 2009 WL 995483, at *10 (Mass. Dist. Ct. Jan. 26, 2009).

95. *See* Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 962 (N.D. Ill. 2009); M.A. *ex rel.* P.K. v. Vill. Voice Media Holdings, LLC, 809 F. Supp. 2d 1041, 1043–46 (E.D. Mo. 2011).

Traditionally, brick-and-mortar establishments[96] incur criminal liability for knowingly facilitating criminal activity.[97] For example, knowingly hosting or profiting from explicit criminal activity is commonly chargeable under an accessory theory attached to the underlying crime.[98] Even if a physical establishment could flout criminal liability by avoiding knowledge of the criminal activity, it would nevertheless incur civil liability from both public and private actors for negligently contributing to the illegal activities.[99] In this way, criminal and civil liability could potentially serve as a disincentive for physical establishments that otherwise might have facilitated criminal activity. However, as more physical establishments move their activities to the Internet, they leave behind much of the liability previously assumed under the brick-and-mortar model. And with that transition, law enforcement's ability to enforce criminal statutes is steadily eroding.

B. Section 230's Assimilation of Distributor Liability

From the outset, section 230 "upended a set of principles enshrined in common law doctrines that had been developed over decades, if not centuries, in cases involving offline intermediaries."[100] Section 230's enactment abruptly extinguished forms of civil liability for intermediaries that hosted and disseminated tortious content—that much is obvious.[101] More insidious, however, is how section 230 obviates various models of criminal liability.[102] Numerous criminal theories of liability that traditionally held intermediaries accountable for contributing to unlawful activity are increasingly subsumed into the general immunities conferred by section 230.[103] This dynamic is exacerbated with the in-

96. By brick-and-mortar establishments, this Comment refers to the physical equivalent of an entity that can now operate entirely online. For example, a traditional newspaper such as the *New York Times* is a brick-and-mortar publisher and is subject to the full battery of legal liability for the content they publish and distribute to the public.

97. *See* MODEL PENAL CODE § 2.06 (2011) (describing the criminal liability incurred by persons or entities that facilitate criminal activity).

98. *Id.*

99. *See* RESTATEMENT (SECOND) OF TORTS § 577(2) (1977) (describing the liability incurred by distributors who continue to exhibit unlawful material).

100. Ardia, *supra* note 8, at 411.

101. *Id.*

102. *See generally* Lawrence G. Walters, *Shooting the Messenger: An Analysis of Theories of Criminal Liability Used Against Adult-Themed Online Service Providers*, 23 STAN. L. & POL'Y REV. 171 (2012).

103. *See* Lukmire, *supra* note 21, at 395–99.

creased migration of criminal activity to online intermediaries dedicated to hosting unlawful content.[104]

The most obvious civil liability that section 230 removed—indeed the most intended in the CDA's enactment—is tortious theories of publisher liability.[105] In fact, the legislative history of section 230 clearly indicates Congress's intent to immunize ICSPs engaged in good faith publishing efforts as well as those who serve merely as passive conduits of third-party created content.[106] However, given early courts' sweeping application of section 230's open-ended language, the courts also subsumed another form of civil liability into the section's immunity granting provision: distributor liability.[107]

Distributor liability pertains to entities that host and disseminate content to the public. Specifically, an entity that distributes content can be held liable if it knows or has reason to know of the content's tortious or illegal nature.[108] Once a distributor knows or has reason to know that the content it is disseminating is unlawful, it must either cease providing the material or incur liability.[109] In the intermediary context, the second form of intermediary (those that host and disseminate online content) would normally be subject to traditional distributor liability.[110] This differs from the first and third category of intermediaries (physical infrastructure providers and passive conduits), which take no affirmative actions to distribute content.[111]

Similar to the subtle distinctions between the three types of online intermediaries,[112] the distinctions for content hosts between publication and distribution liability is sometimes ambiguous. Section 230 was clearly intended to remove the disincentive for online intermediaries to engage in any publishing functions with respect to the content they host.[113] Thus, an online intermediary can engage in good faith efforts "to restrict access to or availability of" offensive material without incurring the

---

104. *See supra* Part III.B.

105. This proposition is demonstrated by the very text of section 230(c)(1), which states, "[n]o provider or user of an interactive computer service shall be treated as the *publisher* or *speaker* of any information provided by another information provided by another information content provider." 47 U.S.C. § 230(c)(1) (1996) (emphasis added).

106. *See supra* Part II.A.

107. *See* Lukmire, *supra* note 21, at 402–05.

108. *See* Ardia, *supra* note 8, at 397–98.

109. *Id.*; *see also* RESTATEMENT (SECOND) OF TORTS § 577(2) (1977) (describing the liability incurred by distributors who continue to exhibit unlawful material).

110. *See supra* Part III.B.

111. *See supra* Part III.B.

112. *See supra* Part III.B.

113. *See* source cited *supra* note 8 and accompanying text.

normal liabilities associated with publishing content.[114] There is no indication, however, that section 230 was intended to immunize distributive activities by online intermediaries.[115] Distribution differs from publishing in that, while publishing is focused on the editorializing of the contents substance, distribution is concerned with optimizing the dissemination of the content to viewers.[116] On its face, section 230's entire focus is on immunizing good faith publishing functions.[117] Nevertheless, courts' overly broad application of section 230(c) consistently ignores the inherent distinction between publishing and distribution and instead applies blanket immunity to a broad range of claims.[118]

Judicial misapplications of section 230 immunity to ICSPs engaged in the distribution of tortious content have obviated the entire field of distributor liability.[119] Some commentators view this as an acceptable consequence "in facilitating the development of . . . modified exceptionalism encourag[ing] 'collaborative production' and the emergence of 'non-commodified digital space that facilitates communication.'"[120] In other words, the "exceptional" benefits the Internet provides justify a largely hands-off regulatory approach.[121] And perhaps that reasoning is correct, especially given the effect the CDA has in enabling the proliferation of communication.[122] However, the collateral consequence of subsuming distributor liability into section 230 immunity is beginning to yield unacceptable consequences, particularly with regard to various criminal theories of liability that share the same elemental principles of culpability as distributive liability.

C. Section 230's Preemption of State's Traditional Police Powers

The courts' extension of section 230's immunity granting provision to distribution theories of civil liability inherently implicates complicity

---

114. 47 U.S.C. § 230(c)(A) (1996).

115. *See* Lukmire, *supra* note 21, at 381–86; David R. Sheridan, Zeran v. AOL *and the Effect of Section 230 of the Communications Decency Act Upon Liability for Defamation on the Internet*, 61 ALB. L. REV. 147, 162 (1997) ("[O]ne could argue from the enumeration of publisher and speaker liability in § 230(c)(1) that distributor liability was deliberately omitted.").

116. *See* Sheridan, *supra* note 115, at 161–63.

117. *See supra* note 105 and accompanying text.

118. Lukmire, *supra* note 21, at 395.

119. *See id.* at 402–05.

120. H. Brian Holland, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, 56 U. KAN. L. REV. 369, 391 (2008) (asserting that section 230 embodies a form of "CyberLibertarian Exceptionalism").

121. *Id.*; *see also* Walters, *supra* note 102, at 212 (claiming that online intermediaries are, "at most, passive conduits of information").

122. *See* Holland, *supra* note 120, at 386–88.

theories of criminal liability. "Complicity" represents a foundational element of criminal liability that shares the basic theories of culpability as distributor liability in the civil context.[123] Specifically, complicity theories are supported by the concept that having actual or constructive knowledge of illegal conduct confers criminal liability on actions taken that enable or further the criminal activity.[124] For example, it is a crime in many states to knowingly engage in conduct that aids or facilitates prostitution,[125] and normally an enterprise that actively facilitates commercial sex advertising could be subject to criminal liability.[126] However, if such an enterprise moves its activities online, in the form of an intermediary content provider, it flouts normal criminal liability under section 230. This is because the immunity granting provision contained in section 230(c) is wrongly interpreted by courts to preempt state laws that seek to hold the ICSPs liable for the elicit content and activity they knowingly host.

Section 230 preempts "any State or local law that" seeks to impose liability inconsistent with the immunity section 230 affords.[127] Courts applying this preemptive provision largely accept the *Zeran* court's interpretation that section 230 broadly immunizes websites from forms of "tort-based lawsuits" and "tort liability."[128] This combination opens the doors for an application of section 230 immunity to various forms of state and local complicity theories of criminal liability thereby preempting the entire field of otherwise applicable law. And given the increasing amount of traditional crimes being facilitated via online intermediaries,[129] broad application of section 230 immunity is progressively obstructing historic police powers.

States are frustrated. Tired of capitulating the invulnerability of certain forms of criminal activity that had migrated to the Internet, some states have attempted to expand criminal liability to online intermediaries facilitating criminal activity on the Internet. For example, in Washington State, legislators passed a bill that criminalized the act of hosting com-

123. *Compare* MODEL PENAL CODE § 2.06 (2011), *with* RESTATEMENT (SECOND) OF TORTS § 577(2) (1977).

124. *See, e.g.*, N.Y. PENAL LAW § 115.00 (1978); ARIZ. REV. STAT. ANN. § 13-1004 (2012).

125. *See, e.g.*, WASH. REV. CODE § 9A.88.060 (2011).

126. *See* MODEL PENAL CODE § 2.06 (2011).

127. 47 U.S.C. § 230(e)(3) (1996).

128. Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997); *see also* Lukmire, *supra* note 21, at 395.

129. *See supra* Part III.A.

mercial sex advertisements involving a minor.[130] The provisions of the bill essentially imposed strict liability on ICSPs that hosted commercial sex advertisements depicting minors, which could only be overcome by a showing of "bona fide" efforts to ascertain the age of the individual depicted.[131] Another state followed suit by introducing similar legislation designed to expressly criminalize websites that actively advertised commercial sex.[132] The Washington law was quickly challenged by ICSPs claiming it was preempted by section 230[133] and that it violated the First Amendment and the Commerce Clause.[134] A federal district court agreed and issued a preliminary injunction enjoining the law's enforcement in July 2012.[135] According to the court decision, Washington's unsuccessful attempt to impose criminal liability on websites advertising minors for commercial sex was clearly incongruent with section 230.[136] However, the bill does represent a growing frustration—if not desperation—by

130. Senate Bill 6251 was scheduled to take effect on June 7, 2012, and essentially extended criminal liability to websites which hosted commercial sexual advertisements depicting a minor. The relevant provisions of the bill are as follows:

> (1) A person commits the offense of advertising commercial sexual abuse of a minor if he or she knowingly publishes, disseminates, or displays, or causes directly or indirectly, to be published, disseminated or displayed, and advertisement for a commercial sex act, which is to take place in the state of Washington and that includes the depiction of a minor . . . .
>
> (2) In a prosecution under this statute, it is not a defense that the defendant did not know the age of the minor depicted in the advertisement. It is a defense, which the defendant must prove by a preponderance of the evidence, that the defendant made a reasonable bona fide attempt to ascertain the true age of the minor depicted in the advertisement by requiring, prior to publication, dissemination, or display of the advertisement, production of a driver's license, marriage license, birth certificate, or other governmental or educational identification card or paper of the minor depicted in the advertisement.

S.B. 6251, 62d Leg., Reg. Sess. (Wash. 2012).

131. *Id.*

132. Specifically, the Tennessee legislature passed a similar law to the Washington bill. *See* TENN. CODE. ANN. § 39-13-315 (2012). However, the Tennessee law was soon challenged in federal court and subsequently enjoined from enforcement. *See* Order Granting Plaintiff's Motion for Preliminary Injunction, Backpage.com, LLC v. Cooper, No. 3:12-cv-00654, 2013 WL 1249063, at *2 (M.D. Tenn. 2013).

133. *See* Order Granting Plaintiff's Motion for Permanent Injunction, Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262, 1271 (W.D. Wash. 2012).

134. *Id.* at 1275–86. In many respects, the bill was just like the older provisions of the CDA that were struck down by the Supreme Court in *Reno v. ACLU*.

135. *Id.* at 1265.

136. As the court in *Backpage.com* stated,

> SB 6251 is inconsistent with Section 230 because it criminalizes the 'knowing' publication, dissemination, or display of specified content. In doing so, it creates an incentive for online service providers *not* to monitor the content that passes through its channels. This was precisely the situation that the CDA was enacted to remedy.

Id. at 1273 (citing Batzel v. Smith, 333 F.3d 1018, 1029 (9th Cir. 2003)).

state and local governments to combat the increasing amount of criminal activity finding safe refuge on the Internet.

As more and more criminal activity migrates to the Internet and with the apparent difficulty for states to criminalize complicity by intermediaries, section 230's preemptive effect on traditional state laws is mounting. These civil and criminal laws stand at the heart of state's historic police powers. Surely this was not Congress's intent when it enacted section 230. Nonetheless, if this trend continues, the states' ability to combat criminal activity will continue to erode, and with it, a fundamental component of their sovereignty.

IV. RENEWING THE PRESUMPTION AGAINST PREEMPTION

Modern courts applying section 230 immunity frequently accept the broad preemptive effect given to the statute by earlier courts. Missing from virtually every court's analysis is a presumption *against* section 230's preemption of traditional state police powers in non-publisher contexts. Were courts to reexamine Congress's preemptive intent, it would quickly become apparent that section 230 was only intended to override publisher theories of liability. As illustrated below, this is evident from both the text of section 230 as well as the legislative history and purpose.

While Congress generally has broad authority to regulate the Internet, it does not necessarily follow that courts should give section 230 the broadest possible effect. The Internet simultaneously embodies a channel,[137] article,[138] instrumentality,[139] and activity substantially affecting interstate commerce.[140] Accordingly, Congress generally has broad authority under the Commerce Clause to regulate the Internet, and any such regulation will preempt "state laws that interfere with, or are contrary to, federal law."[141] But the mere ability of Congress to regulate the Internet does not necessarily preempt concurring state regulation.[142] Even if Congress acts, courts should maintain a presumption against preemption ab-

137. *See, e.g.*, Heart of Atlanta Motel, Inc. v. United States, 379 U.S. 241, 357 (1964).

138. *See, e.g.*, E. & W.T.R. Co. v. United States, 234 U.S. 342 (1914).

139. *See, e.g.*, United States v. Lopez, 514 U.S. 549, 558 (1995).

140. *See, e.g.*, NLRB v. Jones & Laughlin Steel Corp., 301 U.S. 1, 37 (1937).

141. Hillsborough Cnty. v. Automated Med. Labs, Inc., 471 U.S. 707, 712 (1985) (internal quotation marks omitted).

142. *See* Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785, 787 (2001) (arguing that the states retain "flexibility to regulate Internet" despite its obvious categorization as interstate commerce). Professors Goldsmith and Sykes argue against the categorical presumptions by earlier commentators that *any* local regulation of the Internet represented a violation of the Dormant Commerce Clause. *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095, 1123–34 (1996).

sent a showing of Congress's "clear and manifest" intent to invalidate local regulation.[143] A court's "ultimate task" in determining whether a federal law preempts a local regulation is to decide whether the local law is consistent with the "structure and purpose" of the federal statute.[144] In application, a court's conflict inquiry is "guided by two cornerstones of . . . pre-emption jurisprudence."[145] First, "the purpose of Congress is the ultimate touchstone in every pre-emption case."[146] Second, courts assume "that the historic police powers of the States [are] not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress."[147]

In determining the first cornerstone—Congress's preemptive intent—courts will look for either an express preemption provision within the statute or a clear conflict in which state law frustrates the federal statutory purposes or objectives.[148] Turning back to section 230, Congress expressly articulated the preemptive scope of the statue as it pertains to state law: "Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[149] Unfortunately, this language is entirely self-referencing and essentially directs courts to engage in the second cornerstone analysis identified above: identifying impliedly preempted statutes.[150]

A plain language reading of section 230 and its legislative history implies that Congress only intended to preempt State laws that imposed publisher liability. Identifying the purpose of Congress necessitates a broader inquiry into Congress's general intent by enacting the statute.[151]

---

143. Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947).

144. Gade v. Nat'l Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 98 (1992); *see also* Gibbons v. Ogden, 22 U.S. 1, 211 (1824) ("[T]hough enacted in the execution of acknowledged State powers, [laws that] interfere with, or are contrary to the laws of Congress . . . must yield to [federal law].").

145. Wyeth v. Levine, 555 U.S. 555, 565 (2009).

146. *Id*. (quoting Medtronic, Inc. v. Lohr, 518 U.S. 470, 485 (1996)).

147. *Lohr*, 518 U.S. at 485 (quoting *Rice*, 331 U.S. at 230) (internal quotation marks omitted). Intrinsically, the presumption against preemption of state's traditional police powers resonates of this country's thematic notion of federalism and inherent state sovereignty and, therefore, should be maintained in every instance. *See* Robert S. Peck, *A Separation-of-Powers Defense of the "Presumption Against Preemption,"* 84 TUL L. REV. 1185, 1196 (2010).

148. *See* Hines v. Davidowitz, 312 U.S. 52, 66–68 (1941); Ernest A. Young, *"The Ordinary Diet of the Law": The Presumption Against Preemption in the Roberts Court*, 2011 SUP. CT. REV. 253, 270–72 (2011).

149. 47 U.S.C. § 230(e)(3) (1996).

150. *See* Young, *supra* note 148, at 273–76.

151. Wyeth v. Levine, 555 U.S. 555, 556 (2009).

Thankfully, this inquiry is short, since Congress expressly articulated the policies underlying section 230:

> (b) Policy
>
> It is the policy of the United States—
>
> (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
>
> (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
>
> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
>
> (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate material; and
>
> (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassing by means of computer.[152]

Essentially, Congress's purposes for enacting section 230 can be loosely categorized into three separate policy goals. First, Congress wanted to keep the Internet largely deregulated and allow the current online economy to continue to grow unhindered.[153] Next, Congress intended to overturn the *Stratton Oakmont* ruling and remove the disincentive for websites to exercise any efforts at removing offensive content from their site.[154] Finally, Congress intended to ensure decency on the Internet.[155]

Considering the three distinct policy aims of Congress, section 230 does not preempt the entire field of online regulation leaving nothing for states.[156] Specifically, Congress's purpose was to preempt state and local laws that imposed civil liability for websites that took voluntary efforts to remove offensive material provided by third parties—by focusing on

---

152. 47 U.S.C. § 230(b)(1)–(5) (1996).

153. *See supra* Part II.A–B. (discussing the Cox–Wyden proposal's aim in the overall statutory framework of Senator Exon's CDA).

154. *See supra* note 26 and accompanying text.

155. *See generally* Cannon, *supra* note 15.

156. Any state is free to enforce state laws so long as such laws are "consistent with this section." 47 U.S.C. § 230(e)(3) (1996).

publisher liability.[157] This purpose was "clear and manifest" given the express policy aims contained in section 230(b), the explicit strictures of immunity formulated in 230(c), and the circumstantial context of Congress's response. [158]

Initially, courts only struck down the laws that Congress intended to preempt. Because the early courts applying section 230 were largely dealing with factual circumstances similar to those originally envisioned by section 230's drafters, their preemption analysis of conflicting state and local laws was fairly straightforward. [159] As preemption analysis of traditional publisher liability laws was the express aim of section 230,[160] courts generally accepted the preemptive effect when analyzing inconsistent state laws.[161]

Unfortunately, as the Internet continued to grow, section 230 was invoked in more and more circumstances outside of those initially envisioned by the drafters. For example, the district court in *Roommates* erroneously applied section 230's publisher immunity to the defendant ICSP for conduct that amounted to content creation and dissemination.[162] And in *Barnes v. Yahoo!, Inc.*, the Ninth Circuit reversed a district court ruling that the CDA precluded a promissory estoppel claim after the defendant-website promised to remove a fake profile of the plaintiff but then failed to do so.[163] Specifically, the *Barnes* court determined that the district court was correct in applying section 230 immunity to the plaintiff's claims that the website had a duty to remove the offensive content; however, the CDA did not cover promissory estoppel arising from the website's voluntary commitment to remove the posting.[164]

The cases outlined above demonstrate how courts often accept the broad preemptive effect that early courts assigned to section 230(c) and infrequently examine the individual claims involved. That is, courts sel-

157. *Id.*; *see* Sheridan, *supra* note 115, at 151–52.

158. Congress was specifically responding to the *Stratton Oakmont* ruling in an effort to avoid similar circumstances in the future. *See supra* note 26 and accompanying text.

159. Specifically, early courts applied section 230 immunity in instances where a website was being sued by a private individual seeking to impose a form of publisher liability on the website for hosting or providing a means of distribution of defamatory or otherwise offensive content. *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997); Carafano v. Metrosplash, Inc., 339 F.3d 1119, 1121 (9th Cir. 2003); Ben Ezra, Weinstein, & Co., v. Am. Online Inc., 206 F.3d 980, 983 (10th Cir. 2000); Blumenthal v. Drudge, 992 F. Supp. 44, 46 (D.D.C. 1998).

160. *See* 47 U.S.C. § 230(c)(1) (1996).

161. *See supra* note 48 and accompanying cases.

162. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1157 (9th Cir. 2008).

163. *See* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1096 (9th Cir. 2009).

164. *Id.*

dom engage in a refreshed inquiry into whether or not the facts and circumstances of a case are consistent with the limited scope and preemptive context in which Congress intended section 230 to operate. Instead, courts accept broad articulations of section 230's preemptive effect with little thought to the impact of the changing circumstances on the Internet. What is actually warranted in cases alleging non-publisher theories of liability is a renewed inquiry into Congress's preemptive intent, replete with a presumption against preemption.

Also missing from current courts' application of section 230 is the presumption against preemption of traditional state police powers. The obvious effect is that increasingly more criminal activity finds a safe haven on websites dedicated to facilitating unlawful activity. This is largely avoidable because a renewed inquiry into the preemptive effect of section 230 would reveal that Congress did not intend to immunize websites engaged in blatantly criminal activity. Criminal activity does not serve any of the three general policy goals stated in the statute: Specifically, an ICSP that hosts a significant amount of cybercrime does not help drive the growth of the online economy (at least not the legal online economy). Those ICSPs do not engage in good faith efforts to remove objectionable content from the Internet,[165] but are instead in the business of hosting and disseminating objectionable content. And they most certainly do not comport with the overarching statutory framework of the CDA.[166] As such, courts should stop presuming preemption in all section 230 cases, and instead examine the text of section 230 and Congress's intent to preempt state laws.

V. SOLUTIONS

Even if courts engage in a renewed analysis of section 230's preemptive effect and conclude that Congress did not intend to preempt a given state law, they will still be faced with determining to what extent a

165. For example, certain websites engage in filtering or blocking of limited offensive or unlawful content only in an effort to avoid criminal liability for themselves and their unlawful users. This is clearly not out of a good samaritan desire, but is instead motivated purely out of a desire to maintain the profitability of their site. Not only is this blatantly outside of the policy aims of section 230, but it is also explicitly outside of the immunity-granting provision which state "efforts taken in good faith" are immune from civil liability. 47 U.S.C. § 230(c)(2) (1996). Notice also that the very title of this subsection is "Civil Liability," further evidencing the conclusion that Congress was not expecting the provision to serve as a shield for criminal activity of any kind. Curiously, courts have not paid much attention to this clear contradiction despite the unequivocal requirement in the very title of the immunity-granting provision—"Protection for 'good samaritan' blocking and screening of offensive material." 47 U.S.C. § 230(c) (1996). For a discussion of potential judicial remedies for this misconstruction, see *infra* Part V.A.

166. *See supra* Part II.A.

defendant website should be held liable. This is necessitated by the fact that most websites perform entirely innocuous distribution functions and are only misappropriated by third party users bent on unlawful activity. Thus, courts need to craft a doctrine for determining when websites are merely hijacked by unlawful third-party users as opposed to when websites are themselves complicit in illegal activity. Inherently, any judicial remedy will suffer from inconsistency, and given the dynamic and evolving nature of the Internet, new legislation will eventually be imperative.

A. A Judicial Band-Aid

As section 230's immunity granting provisions continue to encroach into the traditional zone of state police power, courts will be faced with a choice of either applying broad immunity, contradicting Congress's intended scope, or fashioning creative construction of section 230 to avoid this conflict. However, because courts can and should construe federal statutes and regulatory schemes to preserve historic state police powers,[167] it is only a matter of time until the current broad immunity-granting interpretations fall away, leaving a much more restricted construction.[168] As previously mentioned, several courts have already begun to construe section 230 in a narrower manner, abandoning the expansive reading originally given to the statute in *Zeran*.[169]

Beginning with *Roommates*,[170] an expansive reading of "develop in part" would remove ICSPs that assume distributor-like roles to facilitate criminal activity from section 230(c)'s grant of immunity.[171] However, this reading of section 230 is not problem-free. In essence, the expansive reading of the word develop, as articulated in *Roomates*, would serve to remove nearly all forms of distributor liability from section 230 immuni-

---

167. *See* Medtronic, Inc. v. Lohr, 518 U.S. 470, 485 (1996).

168. *See* Lorillard Tobacco Co. v. Reilly, 533 U.S. 525, 590–604 (2001) (Stevens J., dissenting) (citations omitted).

> As the regulations at issue in this suit implicate [powers] that lie at the heart of the States' traditional police power . . . our precedents require that the Court construe the preemption provision 'narrow[ly].' If Congress'[s] intent to pre-empt a particular category of regulation is ambiguous, such regulations are not pre-empted. . . . [T]he scope of a pre-emption provision must give effect to a 'reasoned understanding of the way in which Congress intended the statute and its surrounding regulatory scheme to affect business, consumers, and the law.'

Id. at 591–92 (citation omitted).

169. *See supra* Part II.B.

170. *See supra* Part II.B; *see also* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1168–70 (9th Cir. 2008).

171. *See* Weslander, *supra* note 62, at 293–96; *see also* Doty, *supra* note 65, at 129–32 (discussing how the *Roommates* court extrapolated the "underlying illegality" test from it's construction of the term "development" contained in section 230).

ty. While this would be more in accord with the original aims of section 230 set out by Congress,[172] it certainly would not be a practical solution given the enormous burden it would place on legitimate websites and the dampening effect it would have on free speech.[173] Instead, a more nuanced approach is appropriate—one that would not subject to liability the majority of legitimate online intermediaries that are merely misappropriated by third parties to unlawful ends.

The court in *Roommates* articulated an "underlying illegality" test to operate in tandem with its expansive interpretation of section 230's development language.[174] This component preserves the broad grant of immunity for the vast majority of websites, while exposing to liability only those websites that somehow "contribute[] materially to the alleged illegality of the conduct."[175] The problem with this test is in its application. Some courts have adopted a more discernable "solicitation standard," which only voids section 230 immunity if websites explicitly invite unlawful content or activity from third parties.[176] However, this approach allows websites to flout both civil and criminal liability by avoiding express solicitations, and instead, resorting to more subtle and tacit invitations. At the other end of the spectrum, some courts have employed an "inducement" standard whereby a website is excluded from immunity when it engages in conduct that encourages third parties to behave unlawfully.[177] The inducement standard is preferable to the solicitation standard in its ability to exclude immunity from websites that maintain a mere rouse of legitimacy. However, it could become subject to overapplication absent an objective inquiry into the knowledge and intent of the ICSP.

The most comprehensive judicial solution to properly limiting section 230's immunity centers around an objective bad faith exception.[178] This exception would essentially begin with the inducement analysis outlined above, but it would only void immunity upon a showing that the defendant-website was acting in bad faith. In most instances, this would have to be objectively inferred from the website's conduct. For example,

---

172. Specifically, it would remove many forms of distributor liability from the grant of immunity and restore the focus of the provision on publisher functions.

173. *See* Lukmire, *supra* note 21, at 404–05 and authorities cited therein.

174. *Roommates.com*, 521 F.3d at 1167–68; Doty, *supra* note 65, at 129–32.

175. *Roommates.com*, 521 F.3d at 1167–68.

176. *See* Doty, *supra* note 65, at 132–37 and cases cited therein.

177. *Id*. at 136–42.

178. Lukmire, *supra* note 21, 407–11 ("An implied bad faith exception to section 230 immunity for distributors of defamatory content would allow more plaintiffs with meritorious claims to prevail, and would be easier to implement and administer.").

bad faith can be inferred from affirmative actions to enhance the content's unlawfulness, such as creating financial incentives; reducing the risk of detection by law-enforcement; creating webpages devoted to illegal content; and providing tools specifically designed for the illegal content. Implied incentives, such as deriving substantial financial gain from the unlawful content, would also evidence bad faith on the part of website.

The proposed bad faith exception would seriously limit the application of section 230 immunity to websites engaged in unlawful activity and allow states to employ more proactive measures targeting these intermediaries. However, short of a Supreme Court decision that comprehensively articulates this standard, any judicial remedy will inherently suffer from inconsistency in application and jurisdiction among states. Eventually, it will become necessary for Congress to amend or replace section 230 with a more agile statutory scheme aimed at preserving freedom of information on the Internet while still allowing states to combat criminal activity.

B. The Eventual Legislative Imperative

The most obvious solution to avoiding unconstitutional encroachments into state police powers is to enact legislation either amending section 230 or replacing it with a more sophisticated statutory scheme. Given that the majority of commentary on section 230 is from a defamatory view,[179] the most common solutions have drawn from other statutory schemes currently in place. Specifically, several commentators have proposed the Digital Millennium Copyright Act (DMCA) as a viable starting point for modeling a new section 230.[180] Essentially, a DMCA-modeled statute would impose liability on a website for knowingly hosting unlawful content, deriving a benefit attributable to the offending content, and refusing to remove the unlawful content after receiving notice of its illegality.[181] While a DMCA-modeled statute does appear applicable in a defamation context, its requirements of notice and case-by-case removal of individual content make it an impractical solution for allowing law-enforcement agencies to police and shut down websites devoted to hosting illegal activity. At the same time, a statute that imposes traditional "facilitation" liability would unnecessarily exempt from immunity web-

179. *See supra* Part III.B.

180. *See* Colby Ferris, *Communication Indecency: Why the Communications Decency Act, and the Judicial Interpretation of It, Has Led to a Lawless Internet in the Area of Defamation*, 14 BARRY L. REV. 123, 135 (2010); *see also* Lukmire, *supra* note 21, at 406.

181. *See* Ferris, *supra* note 180, at 135.

sites that are occasionally misused for illegal purposes. What is needed is a statute that strikes a balance between the two approaches.

One alternative would be a statute that essentially codifies the objective bad faith principles.[182] However, the text of the statute would have to walk the line between exempting websites that take affirmative steps to disseminate unlawful content and those that serve merely as passive conduits of information. Basically, this would amount to a showing of bad faith on the part of the plaintiff or State, thus maintaining the presumption of immunity. However, upon a showing that the defendant website has taken affirmative actions or otherwise designed its services to invite, encourage, or facilitate unlawful content and activity, the website will no longer be immune from civil or criminal liability.

VI. CONCLUSION

Section 230 of the CDA was enacted to remove the disincentive for online intermediaries to take good faith efforts to monitor and remove offensive content from their websites. Specifically, Congress meant to remove traditional forms of publisher liability and the accompanying legal exposure in the context of defamatory and pornographic content posted by third parties. Thus, Congress intended to preempt any state or local laws that imposed such theories of liability. Unfortunately, early courts interpreting section 230 over-read the scope of immunity provided by the provision and erroneously broadened the range of civil and criminal liability schemes subject to preemption. The negative consequences of this misreading are increasingly felt as more and more criminal activity migrates to the Internet, and the online intermediaries that knowingly host such activity are held immune from traditional modes of checking such lawlessness.

Turning the tide against a lawless no-man's-land on the Internet starts with a reexamination of Congress's intended scope of immunity and the implicit preemptive effect of section 230. Beginning with the presumption that Congress did not intend to preempt an entire field of traditional state police power, and after closely examining the textual components of section 230 as well as the legislative history, it soon becomes apparent that immunity is only applicable in a specific set of circumstances. In applying this analysis, courts could incorporate some form of objective bad faith determination to distinguish between websites that are furthering the purposes of section 230, as opposed to those that are merely posing as good Samaritans. Alternatively, Congress could

182. *See* Lukmire, *supra* note 21, and accompanying text.

clarify the scope of immunity provided to online intermediaries by amending section 230 or enacting a new regulatory scheme all together.