The Never-Ending Limits of § 230: Extending ISP Immunity to the Sexual Exploitation of Children

Katy Noeth*

I. SECTION 230 IMMUNITY 766
A. *Congress's Intent in Enacting § 230* 768
B. *The Seminal § 230 Case and Its Enduring Effects* 768
II. A CASE FOR CHANGING THE § 230 LEGAL REGIME TO PROTECT MINORS ONLINE 770
A. *The Current State of the Law Under § 230* 770
B. *A Multi-Faceted Approach* 772
III. FOUR WAYS TO CURB THE EXTENSION OF § 230 IMMUNITY IN CASES WHERE ISPS KNOWINGLY ALLOW THE SEXUAL EXPLOITATION OF CHILDREN ON THEIR SITES 773
A. *A Congressional Amendment to § 230* 773
B. *Courts Should Distinguish Zeran and Refuse to Apply its Defamation Rationale to Child Sexual Exploitation Claims* 773
C. *Courts Should Recognize that Extending Immunity to ISPs in Child Sexual Exploitation Cases Produces a Result that is Inconsistent with the Original Policy Objectives of Congress in Enacting § 230* 775
1. Imposing the Proposed Liability Will Not Squelch the Growth of the Internet or Create Disincentives for Its Development 776

* J.D. Candidate 2009, Indiana University Maurer School of Law—Bloomington; B.A. History 2005, Indiana University.

2. Imposing the Proposed Liability Will Not Result in an Infeasible Policing of the Internet 778
3. Imposing the Proposed Liability Will Not Inundate the ISPs with Lawsuits 779
D. Courts Should Not Extend § 230 Immunity to a Civil Claim Based on a Violation of § 2252A 781
1. The Exception to § 230 Immunity Provided by § 230(e)(1) and Title 18 U.S.C. § 2252A 781
2. Plaintiffs' Unsuccessful Attempt in *Doe v. Bates* to Bring a Civil Claim Under § 230 Based on an Alleged Violation of Title 18 U.S.C. § 2252A 782
IV. CONCLUSION 784

I. SECTION 230 IMMUNITY

Minors are not safe on the Internet under the current legal regime. Society's obligation to protect its children from sexual predators, wherever they operate,[1] has been hindered by recent judicial determinations, which have held that certain Internet sites are not liable for failing to protect minors from sexual exploitation[2] or assault.[3] These judicial interpretations have rendered Internet Service Providers (ISPs) virtually judgment proof even when they knowingly allow the sexual exploitation of children on their sites.

Section 230 of the Communications Decency Act (CDA) provides immunity[4] to ISPs.[5] It bars claims against ISPs based on the publication of

---

1. *See, e.g.*, Michael D. Marin & Christopher V. Popov, Doe v. MySpace, Inc.: *Liability for Third Party Content on Social Networking Sites*, COMM. LAWYER, Spring 2007, at 3, *available at* http://www.vinson-elkins.com/uploadedFiles/VEsite/Resources/Marin-Popov.pdf.

2. *See* Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 (E.D. Tex. Dec. 27, 2006).

3. *See* Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007), *aff'd*, 528 F.3d 413 (5th Cir. 2008).

4. 47 U.S.C. § 230 (2000). The statute provides: "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." § 230(c)(1).

5. Courts have considered ISPs to be an interactive computer service. *See* Doe v. MySpace, Inc., 474 F. Supp. 2d at 848 (explaining that ISP is defined as a Web site that "functions as an intermediary by providing a forum for the exchange of information between third party users"). In addition, § 230(f)(2) provides:

> Interactive computer service[:] The term "interactive computer service" means 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 educational institutions.

§ 230(f)(2); *see also* § 230(f)(3) ("Information content provider[:] The term 'information content provider' means any person or entity that is responsible, in whole or in part, for the

third-party content. Defendants are immune from liability from state law claims if:

> (1) [They are] a "provider or user of an interactive computer service"; (2) the claim is based on "information provided by another information content provider"; and (3) the claim would treat [the Defendants] "as publisher or speaker" of that information.[6]

There is, however, an exception to this immunity given in § 230(e).[7] It provides: "[n]othing in this section shall be construed to impair the enforcement of section 223 or 231 of this Act, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute."[8]

If civil liability is imposed on Web sites such as Yahoo!, § 230 immunity provides that it must be imposed on the individual posters of content.[9] Courts have typically held that § 230 grants ISPs complete immunity from both publisher and distributor liability.[10] As a result, ISPs including Web sites such as Yahoo!, Google, and MySpace enjoy a "robust" immunity from civil liability under § 230 of the CDA.[11] The extension of CDA immunity under § 230 in recent judicial decisions has served to protect ISPs at the expense of the safety of minors. Courts have missed an opportunity to finally curb the extension of § 230 immunity, and instead, further extended immunity to ISPs who knowingly violate criminal law. As a result, the so-called "decency act" has "been transformed from an appropriate shield into a sword of harm and extreme danger which places technology buzz words and economic considerations above the safety and general welfare of our people."[12]

Under this Note's proposed changes, ISPs such as Yahoo! should be held liable for knowingly allowing the sexual exploitation of children on their sites. This Note will discuss the background of § 230 immunity and several recent judicial developments. It will then explain why a change to the current law is needed and how to effectuate such a change.

---

creation or development of information provided through the Internet or any other interactive computer service.").

6. Universal Comm. Sys. v. Lycos, Inc., 478 F.3d 413, 418 (1st Cir. 2007) (quoting § 230).

7. The CDA grants immunity from all civil liability with certain exceptions expressly laid out in the statute: (1) federal criminal law, (2) intellectual property law, (3) state law that is consistent with this section, and (4) the Electronic Communications Privacy Act of 1986. *See* Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).

8. § 230(e)(1).

9. *See* David V. Richards, *Posting Personal Information on the Internet: A Case for Changing the Legal Regime Created by § 230 of the Communications Decency Act*, 85 TEX. L. REV. 1321, 1337 (2007) (offering six alternative solutions to § 230 immunity).

10. *See id.* at 1336.

11. Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003).

12. Doe v. Am. Online, Inc., 783 So. 2d 1010, 1019 (Fla. 2001) (Lewis, J. dissenting).

A. Congress's Intent in Enacting § 230

The legislative purpose behind enacting § 230 in 1996 was to ensure that the threat of litigation would not discourage the growth and development of the Internet and other online services.[13] The legislative history surrounding Congress's creation of § 230 reflects the desire to protect online intermediaries from liability for unlawful third-party content.[14] Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.[15] Congress found that:

> (1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.
>
> (2) These services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops.
>
> (3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.
>
> (4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.
>
> (5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.[16]

Congress reasoned that any liability would threaten development of the online industry as a medium for new forms of mass communication and would simultaneously create disincentives for self-regulation by service providers.[17] Congress enacted § 230 to prevent this unwanted result.

B. The Seminal § 230 Case and Its Enduring Effects

The seminal case on § 230 immunity is *Zeran v. America Online, Inc.*[18] The case arose when America Online (AOL) failed to remove a defamatory posting on its site.[19] The plaintiff, Zeran, contended that once he had notified AOL of the defamatory posting, AOL had a "duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory

---

13. *See* § 230(b)(1), (2), (4).

14. *See* Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 (E.D. Tex. Dec. 27, 2006).

15. *See Carafano*, 339 F.3d at 1122-24 (quoting Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997)).

16. *See* § 230(a).

17. *See id.*

18. 129 F.3d 327 (4th Cir. 1997).

19. *See id.* at 327.

material."[20] The Fourth Circuit Court of Appeals disagreed with Zeran and found that § 230 barred his claim.[21]

The court held that § 230 "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[22] It explained that, "both the negligent communication of a defamatory statement and the failure to remove such a statement when first communicated by another party . . . constitute publication."[23] In so finding, the Fourth Circuit extended § 230 immunity to ISPs (here, AOL) that failed to withdraw content *despite having prior notice* of the content's unlawful nature.[24] The court reasoned that the decision to publish, withdraw, postpone, or alter content is a traditional editorial function of a publisher, the exercise of which cannot be a basis for liability under the CDA.[25]

This rationale has endured and has played a critical role in courts' decisions in subsequent CDA cases. Courts have extended the *Zeran* court's rationale for granting immunity to non-defamation claims related to the publication of third-party content and the harms resulting from such publication.[26] As a result of these courts' decisions, ISPs have "no obligation to remove tortious materials, to prevent the reposting of objectionable materials, or to help victims track down the primary wrongdoers."[27] The effect of these expansive judicial interpretations of § 230 "has been the emergence of a comprehensive immunity from suit for ISPs so long as the suits are based on content not authored by the ISP."[28] In sum, the "judiciary's inflated interpretation of § 230 has created a legal environment that is ideal for injury and difficult for redress."[29] The end result is that courts have expanded § 230 to immunize ISPs from virtually every tort action.[30]

---

20. *Id.* at 330.
21. *Id.* at 335.
22. *Id.* at 330.
23. *Id.* at 332.
24. *Id.* at 332-33.
25. *Id.* at 330.
26. *See, e.g.*, Ben Ezra, Wienstein & Co., Inc. v. Am. Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000).
27. Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 341 (2005).
28. Paul Ehrlich, *Communications Decency Act § 230*, 17 BERKELEY TECH. L.J. 401, 402, 406-11 (2002).
29. Rustad & Koenig, *supra* note 27, at 341.
30. *See id.* at 342-43.

II. A CASE FOR CHANGING THE § 230 LEGAL REGIME TO PROTECT MINORS ONLINE

A. The Current State of the Law Under § 230

The trend of broadening § 230 immunity continues in a new line of cases. The heart of the plaintiffs' claims in each case is the protection of minors.[31] Protecting ISPs' freedom on the Internet has reached a high point with several recent court decisions, each finding that § 230 shields an ISP from civil liability regardless of whether it attempted to remove the offending material or whether it knew the material existed on its site.[32]

In December 2006, U.S. District Judge David Folsom decided the case *Doe v. Bates*,[33] consistent with Magistrate Judge Caroline Craven's recommendation. The decision extended the immunity of § 230 so that Yahoo! could not be sued for *knowingly profiting* from a site where members exchanged sexually explicit photos of minors.[34] In this case, a young boy's photographs were featured on an illegal pornography e-group[35] called Candyman that was hosted and operated by Yahoo!.[36] The Candyman e-group allowed members to exchange messages and was "a forum for sharing, posting, e-mailing, and transmitting hard-core, illegal child pornography."[37] The plaintiffs (the parents of the child) alleged that Yahoo! knowingly hosted illegal child pornography on its e-group and they contended that it should have prevented, removed, and/or blocked the illegal child pornography from its Web site.[38]

Magistrate Judge Craven found, and Judge Folsom agreed, that Yahoo! knew or had reason to know about the illegal nature of its content because: "(1) the site was in an adult entertainment subcategory, (2) its introductory web page expressly stated that the group was for people who 'love kids,' and (3) *any type* of message, picture, or video could be posted

---

31. *See* Recent Cases, *Internet Law — Communications Decency Act — Texas District Court Extends § 230 Immunity to Social Networking Sites. —* Doe v. MySpace, Inc., *474 F. Supp. 2d 843 (W.D. Tex. 2007)*, 121 HARV. L. REV. 930 (2008) [hereinafter *Internet Law — Communications Decency Act*].

32. *See* Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 (E.D. Tex. Dec. 27, 2006); *see also* Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007).

33. No. 5:05-CV-91, 2006 WL 3813758 (E.D. Tex. Dec. 27, 2006).

34. *See id.* at *3.

35. E-groups are topic-specific forums which allow, encourage, and facilitate e-group members to engage in discussions, share photographs and files, plan events, exchange ideas and information, and nurture interests and activities. *See id.* at *1.

36. *Id.* at *5 (Craven, Mag. J., Report and Recommendation).

37. *Id.* (Craven, Mag. J., Report and Recommendation).

38. *See id.* at *3-4. Plaintiffs filed a civil suit against Yahoo! claiming civil damages under 18 U.S.C. § 2252A for negligence, negligence per se, intentional infliction of emotional distress, invasion of privacy, and civil conspiracy for allegedly allowing the trafficking of illegal child pornography. *See id.* at *1.

on the site."[39] Judge Folsom ruled that § 230 grants ISPs immunity from all private civil liability regardless of their knowledge of the content of an illegal site or whether they profit from the site, reasoning that this type of litigation would have an "obvious chilling effect" on the Internet.[40] Judge Folsom explained that, "[w]hile the facts of a child pornography case such as this one may be highly offensive, Congress has decided that the parties to be punished and deterred are not the Internet service providers but rather those who created and posted the illegal material."[41]

Following this rationale, the Western District of Texas Court of Appeals, in *Doe v. MySpace, Inc.*,[42] cited *Doe v. Bates* in holding that § 230 immunized the social networking site MySpace from claims involving the sexual assault of a fourteen-year-old girl who met her attacker through the Web site. In *Doe v. MySpace, Inc.*, Julie Doe created a profile on MySpace when she was thirteen years old.[43] When she was fourteen, Pete Solis, nineteen years old, initiated contact with her through MySpace.[44] Thereafter, she provided Solis with her contact information and they arranged to meet for a date. On the date, Pete Solis sexually assaulted Julie Doe.[45] U.S. District Court Judge Sparks dismissed the case under § 230 because it was "directed toward MySpace in its capacity as a publisher.[46]

Subsequent to the *Doe v. MySpace, Inc.* decision, the Northern District Court of Appeals of Ohio followed this same line of reasoning in applying immunity to ISPs, even when the suit was not based on their capacity as publisher. In *Doe v. SexSearch.com*,[47] the plaintiff alleged that he mistakenly had sex with a minor he had met through the online dating service because the minor portrayed herself as an adult. At issue was the "fact that a minor was on the SexSearch website, and not, the content of the minor's profile."[48] Instead of evaluating the claim as pled, the court followed the example of *Doe v. MySpace, Inc.* and concluded that the plaintiffs were simply attempting to plead around the CDA.[49] The court explained,

---

39. *Id.* at *6, (Craven, Mag. J., Report and Recommendation) (emphasis added).
40. *Id.* at *4 (quoting Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997)).
41. *Id.*
42. 474 F. Supp. 2d 843 (W.D. Tex. 2007).
43. *Id.* at 846. Although fourteen is the minimum age required by MySpace to use its services, Julie Doe lied about her age and represented that she was eighteen years old. *Id.* at 846, 846 n.3.
44. *Id.* at 846.
45. *Id.*
46. *Id.* at 849.
47. 502 F. Supp. 2d 719 (N.D. Ohio 2007).
48. *Id.* at 727.
49. *Id.*

> [i]n the present action, Plaintiff attempts to do the same thing as the plaintiffs in *Doe v. MySpace*. . . .
>
> At the end of the day, however, Plaintiff is seeking to hold SexSearch liable for its publication of third-party content and harms flowing from the dissemination of that content.[50]

The court found that, because the plaintiff's claims all hinged on SexSearch's failure to remove the girl's profile or failure to prevent her assaulter from communicating with her, their claims were barred under § 230.[51]

These three decisions have begun to lead § 230 jurisprudence down a slippery slope. Defendants have succeeded thus far in these cases on the argument that ISPs cannot be held liable on *any* state or federal claim which would render that service liable for content provided by third parties.[52] Each of these three cases offers similar rationales for extending immunity to the ISPs in cases involving sexual predators: (1) the plaintiffs' claims that the ISPs failed to react properly to discovering the sexual predators on their sites is analogous to the ISPs in *Zeran* discovering the defamatory postings, and so the reasoning in extending immunity to those ISPs is applicable; and (2) from a policy standpoint, it would create an "impossible burden" on the ISPs to act in these situations, and Congress, in passing § 230, intended that ISPs not bear such a burden.[53] Several other suits have been filed by parents accusing MySpace of "failing to prevent pedophiles from using the site to make contact with -- and ultimately molest -- their children."[54] Based on the current condition of the law, it is likely that these claims will fail.

B. A Multi-Faceted Approach

There are several ways to remedy the current trend of decisions and cases, and to comply with both the clear language of § 230 and the legislative intent of Congress in providing ISPs with immunity. Scholars have suggested a variety of ideas for reforming or repealing § 230 immunity.[55] The best approach entails a multi-faceted process.

This Note will focus on four solutions to prevent future courts from following the precedent established by *Doe v. Bates*, *Doe v. MySpace, Inc.*, and *Doe v. SexSearch.com*. Section 230 should be amended to reflect

---

50. *Id.*

51. *Id.* at 727-28.

52. *See, e.g.*, *id.* at 726.

53. *See* Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 848 (W.D. Tex. 2007); *see also* Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997).

54. Annotation, *Court Finds No Room for Suit Against MySpace Over Sexual Assault, Doe v. MySpace*, 24 ANDREWS COMPUTER & INTERNET LITIG. REP. 2 (2007).

55. *See* Richards, *supra* note 9, at 1344-45.

contemporary developments on the Internet to impose civil liability upon ISPs that knowingly allow the sexual exploitation of children on their sites. In the meantime, however, courts should intervene to mitigate the potential harm of continuing down the path of protecting sexual predators by doing three things. First, future courts should distinguish *Zeran* and refuse to apply its defamation rationale to child sexual exploitation claims. Second, courts should refuse to extend the immunity that ISPs attempt to hide behind in child sexual exploitation claims because such immunity does not further congressional intent behind § 230. Third, courts should recognize an exception to immunity and impose liability upon ISPs when they knowingly receive and/or distribute child pornography on their sites under § 230(e)(1).

III. FOUR WAYS TO CURB THE EXTENSION OF § 230 IMMUNITY IN CASES WHERE ISPS KNOWINGLY ALLOW THE SEXUAL EXPLOITATION OF CHILDREN ON THEIR SITES

A. A Congressional Amendment to § 230

The most straightforward approach to prevent decisions similar to *Doe v. Bates*, is a congressional amendment. The language of § 230 should be changed to reflect contemporary developments on the Internet. To that end, I propose the following simple addition to § 230: *Nothing in this Section shall be construed to grant an interactive computer service immunity from civil claims arising under Chapter 110 where the interactive computer service knowingly received or distributed child pornography.*

Although federal legislators should amend the CDA to account for the changing nature of interactive Web sites, "the speed of the Internet's development outpaces that of congressional legislation."[56] Courts should use common sense and face the realities of the current state of affairs in making decisions in order to clarify the legal landscape for ISPs.

B. Courts Should Distinguish Zeran and Refuse to Apply its Defamation Rationale to Child Sexual Exploitation Claims

The *Zeran* court "laid the groundwork" for the *Doe v. Bates*, *Doe v. MySpace, Inc.*, and *Doe v. SexSearch.com* decisions in holding that § 230 bars lawsuits seeking to hold ISPs liable for their exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content.[57] The judges in *Doe v. Bates*, *Doe v. MySpace, Inc.*, and *Doe v. SexSearch.com* similarly refused to hold the

56. *Internet Law — Communications Decency Act*, *supra* note 31, at 936.

57. Roxanne E. Christ & Jeanne S. Berges, *Social Networking Sites: To Monitor or Not to Monitor Users and Their Content?*, 19 INTELL. PROP. & TECH. L.J. 13, 14 (2007).

ISPs liable for failing to police their sites for harmful third-party provided content. These decisions demonstrate the willingness of courts to extend § 230 immunity from defamation suits to child sexual exploitation claims, even when it enables sexual predators to prey on minors. The effect of these decisions is that, by applying the rationale of *Zeran*, ISPs may have *knowledge and warning* about the existence of child pornography and/or sexual predators using their sites, yet continue to enjoy complete immunity from civil suits under § 230.

In reaching his decision in *Doe v. Bates*, Judge Folsom refused to draw a distinction between a child sexual exploitation claim and a typical defamation claim. He held Yahoo! to be immune from liability under § 230 because it played no role in the creation or development of the images.[58] Yahoo! would be held immune *even if* it placed advertising on the Web site or *modified* or *enlarged* the photographs.[59] As Magistrate Craven explained, "[c]hild pornography obviously is intolerable, but civil immunity for interactive service providers does not constitute 'tolerance' of child pornography any more than civil immunity from the numerous other forms of harmful content that third parties may create constitutes approval of that content."[60] The effect of this analogizing of "numerous other forms of harmful content" (here, pornography) to "defamation" was to hold the difference between child pornography and defamation irrelevant for purposes of § 230 immunity.[61]

Judge Sparks, in *Doe v. MySpace, Inc.*, cited *Bates* in supporting his conclusion that the plaintiffs' claims were within the purview of § 230.[62] He analogized the plaintiffs' claims to the claims in *Zeran*.[63] Judge Sparks explained that because MySpace "failed to react appropriately" when it knew that sexual predators were using its service to communicate with minors, and thus "can be analogized to *Zeran*'s claims that AOL failed to act quickly enough to remove the ads and to prevent the posting of additional ads after AOL was on notice that the content was false."[64] Judge Sparks was not persuaded by the plaintiffs' argument that their case was not based on MySpace's posting of third-party content, but rather on MySpace's failure to institute safety measures to protect minors.[65]

---

58. Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758, at *4-5 (E.D. Tex. Dec. 27, 2006).

59. *See* Christ and Burges, *supra* note 57, at 14-15.

60. Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 at *22 (E.D. Tex. Dec. 27, 2006) (Craven, Mag. J., Report and Recommendation).

61. *Id.*

62. Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 849 (W.D. Tex. 2007).

63. *Id.* at 848-49.

64. *Id.* at 848.

65. *Id.*

The facts, policy considerations, and practical implications of the holding and rationale of *Zeran*—a Fourth Circuit Court of Appeals case decided in 1997 shortly after the CDA was enacted—are readily distinguishable from those of *Doe v. Bates*, *Doe v. MySpace, Inc.*, and *Doe v. SexSearch.com*.[66] *Zeran*'s holding does not necessitate the courts' holdings in *Doe v. Bates*, *Doe v. MySpace, Inc.*, and *Doe v. SexSearch.com* that the ISPs are immune from liability for knowingly receiving and/or distributing forms of illegal child sexual exploitation on their Web sites. Even if—as Judge Folsom and Judge Sparks posit[67]—a publisher's role is legally identical in the face of child pornography and defamatory statements, policy considerations should mandate a distinction between *Zeran*'s defamation claim and child sexual exploitation claims. The court in *Zeran* reached its decision through a careful analysis of the CDA's goals, which are much closer to being realized in 2009 than they were in 1997.[68] This Note does not mean to suggest that the reasoning of *Zeran* is unpersuasive. Courts deciding similar cases in the future, however, should acknowledge and consider these distinctions when ruling on child sexual exploitation claims.

C. Courts Should Recognize that Extending Immunity to ISPs in Child Sexual Exploitation Cases Produces a Result that is Inconsistent with the Original Policy Objectives of Congress in Enacting § 230

The policy rationales used by courts to justify the continued expansion of § 230 immunity do not compel an extension of the immunity to ISPs who knowingly act as publishers or distributors of information that results in the sexual exploitation of children. The suggestion that ISPs should be held civilly liable for their roles as distributors and producers has faced criticism, which stems from the fact that § 230 immunity serves to incentivize creation and encourage freedom of expression on the Internet.[69] It has been argued that imposing liability upon ISPs would squelch the growth of the Internet, would call for infeasible "policing" of the ISPs' Web sites, and would create an overload of lawsuits against ISPs—whom they claim are not in the best position to protect minors.[70] These arguments

66. Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997); *see also* Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 148 (2008).

67. *See generally*, Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 (E.D. Tex. Dec. 27, 2006); *see also* Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007).

68. *See infra* Part III.C.1.

69. *See* Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 at *4 (E.D. Tex. Dec. 27, 2006).

70. *See id.*

have proven to be persuasive in the general context of imposing liability on ISPs. However, Congress's goals of freedom and expansion of the Internet are not served by allowing ISPs to knowingly allow and profit from the sexual exploitation of children on their Web sites. Carving out a narrow exception under § 230 to allow a small range of claims against ISPs—holding them liable when they knowingly allow the sexual exploitation of children on their sites—will not undermine congressional intent.

Congress could not have intended to give interactive Web sites the freedom to act without any restraints.[71] The inclusive immunity extended by courts to allow ISPs to go unchecked by the law in this area surely was not what Congress had in mind when it expressed its intent to further the development of the Internet.[72] Judge Lewis accurately summarized the illogicality of this extension:

> the carefully crafted statute at issue, undergirded by a clear legislative history, does not reflect an intent to totally exonerate and insulate an ISP from responsibility where . . . it is alleged that an ISP has acted as a knowing distributor of material leading to the purchase, sale, expansion and advancement of child pornography, after having been given actual notice of the particular activity, by taking absolutely no steps to curtail continued dissemination of the information by its specifically identified customer, when it had the right and power to do so.[73]

An examination of each of the criticisms of imposing liability reveals why they are unpersuasive in the context of extending immunity to ISPs who knowingly allow the sexual exploitation of children on their Web sites.

1. Imposing the Proposed Liability Will Not Squelch the Growth of the Internet or Create Disincentives for Its Development

The relative concerns of the development of the Internet and the increase of child pornography have shifted since § 230's passing. The congressional goal of promoting the development of the Internet has been accomplished to a significant extent. Technological advances have resulted in a drastically advanced cyber world from the one that existed when the CDA was passed in 1996. The landscape and modern realities of the Internet have changed significantly. Internet sites are flourishing,[74] and the

---

71. *See Internet Law — Communications Decency Act*, *supra* note 31.

72. *See* Matthew J. Jeweler, *The Communications Decency Act of 1996: Why § 230 is Outdated and Publisher Liability for Defamation Should Be Reinstated Against Internet Service Providers*, 8 U. PITT. J. L. & POL'Y 3 (2008) (arguing that Web site operators should no longer be able to benefit from an outdated law that was meant to promote the growth of the Internet).

73. Doe v. Am. Online, Inc., 783 So. 2d 1010, 1019 (Fla. 2000) (Lewis, J., dissenting).

74. *See* Richards, *supra* note 9, at 1323.

Internet now serves almost 1.5 billion people.[75] Internet usage increased 129.6% in North America alone from 2000 until 2008, and 305.5% throughout the rest of the world.[76]

The task of curbing the explosion of child pornography on the Internet, on the other hand, has not yet been accomplished. The Department of Justice (DOJ) has stated that "[t]he Internet has escalated the problem of child pornography by increasing the amount of material available, the efficiency of its distribution, and the ease of its accessibility."[77] The interactivity and ease of information sharing on the Internet has increased the quantity of child pornography available because it "permits access to vast quantities of pornographic images from around the world[,] makes pornography instantly available at any time or place[, and] allows pornography to be accessed (apparently) anonymously and privately."[78] It is difficult to estimate precisely the extent of Internet child pornography, but according to the DOJ, "all of the available evidence points to it being a major and growing problem."[79] Available statistics demonstrate the extent of the problem of child pornography on the Internet. For example, the number of Internet child pornography images has increased 1500% since 1988.[80] Child pornography has become a $3 billion-a-year industry,[81] and approximately twenty percent of all Internet pornography involves children.[82] According to the DOJ, at any one time it is estimated that there are "more than one million pornographic images of children on the Internet, with 200 new images posted daily."[83] It has also been reported by the DOJ that "a single child pornography site received a million hits in a month" and that "there are between 50,000 and 100,000 pedophiles involved in organized pornography rings around the world, and that one-third of these operate from the United States."[84]

---

75. World Internet Usage Statistics News and World Population Stats, http://www.internetworldstats.com/stats.htm (last visited Apr. 9, 2009).

76. *Id.*

77. RICHARD WORTLEY & STEPHEN SMALLBONE, U.S. DEP'T OF JUSTICE, CHILD PORNOGRAPHY ON THE INTERNET 8 (2006), *available at* http://www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

78. *Id.*

79. *Id.* at 12.

80. *Internet Child Porn Safety Call*, BBC NEWS, Jan. 12, 2004, http://news.bbc.co.uk/2/hi/technology/3390813.stm.

81. CHILD WISE, CHILD PORNOGRAPHY & THE INTERNET, http://www.childwise.net/downloads/Child_Pornogprahy.pdf (last visited Apr. 9, 2009).

82. Enough is Enough: Making the Internet Safer for Children and Families—Statistics, http://www.enough.org/inside.php?tag=statistics (last visited Apr. 9, 2009).

83. *See* WORTLEY & SMALLBONE, *supra* note 77 at 12 (internal citation omitted).

84. *See id.* at 12-13 (internal citations omitted).

The rise of youth participation in social networking sites also makes minors vulnerable to sexual predators. In 2007, MySpace was the most visited Web site in the United States.[85] Many of the site's users are minors. On a monthly basis, nineteen percent of MySpace users are minors under the age of seventeen.[86] The result of this rise in youth participation is that "[a]s social networking websites target increasingly younger audiences, the need for security will continue to increase."[87]

Moreover, the imposition of civil penalties for knowingly receiving and/or distributing materials that contribute to the sexual exploitation of children will not create disincentives for Internet development because, for this narrow range of claims, criminal disincentives are already in place.[88] Disincentives will exist whether civil liability is possible or not. The Plaintiffs correctly argued in *Doe v. Bates* that "[i]f the prospect of civil liability provides a disincentive for engaging in child pornography over and above that provided by the prospect of fines and jail time, then that is a good thing."[89]

2. Imposing the Proposed Liability Will Not Result in an Infeasible Policing of the Internet

A narrow exception—to impose liability upon an ISP when it knowingly allows the sexual exploitation of children on its site—will not result in prohibitive amounts of monitoring nor will it inhibit communication over the Internet. The "policing" of the Internet envisioned by the court in *Zeran* (had civil liability been imposed on ISPs in that case) would not materialize by imposing liability on ISPs in this narrow range of cases relating to ISPs that knowingly allow the sexual exploitation of children on their Web sites. The court in *Zeran* stated that,

> [t]he amount of information communicated via interactive computer services is . . . staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems.[90]

---

85. Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 845 (W.D. Tex. 2007).

86. Julia Angwin & Brian Steinberg, *News Corp. Goal: Make MySpace Safer for Teens*, WALL ST. J., Feb. 17, 2006, at B1.

87. *See Internet Law — Communications Decency Act*, *supra* note 31, at 934. The article further noted, "[t]he Internet now provides virtual worlds in which children as young as thirteen can meet complete strangers online and quickly proceed to become friends, get 'married,' and even raise virtual children." *Id.* at 937.

88. *See* 18 U.S.C. § 2252 (2008).

89. Plaintiff's Objections to Report and Recommendation by Magistrate Judge Craven at *17, Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 (E.D. Tex. Dec. 27, 2006) [hereinafter Plaintiff's Objections, *Doe v. Bates*], *available at* 2006 WL 813809.

90. Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).

That same reasoning—that imposing civil liability on ISPs would create an impossible burden—prevailed in the *Doe v. Bates* and *Doe v. MySpace, Inc.* cases. Judge Folsom, in *Doe v. Bates*, found that to require ISPs to screen for potentially obscene materials, or even to respond to notices of such materials, would not be feasible because the sheer number of postings would create an "impossible burden" on the provider.[91] Similarly, Judge Sparks, in *Doe v. MySpace, Inc.*, reasoned that,

> [t]o impose a duty under these circumstances for MySpace to confirm or determine the age of each applicant, with liability resulting from negligence in performing or not performing that duty, would of course stop MySpace's business in its tracks and close this avenue of communication, which Congress in its wisdom has decided to protect.[92]

Contrary to the assertions of Judges Folsom and Sparks, the burden imposed upon ISPs would be modest if they were only held liable for knowingly allowing the sexual exploitation of children on their Web sites. The imposition of liability in cases involving ISPs that knowingly allow the sexual exploitation of children on their Web sites,[93] would not result in the impractical burden imposed upon ISPs in the traditional defamation cases. A duty to monitor everything that comes across an ISP's Web site may in fact inhibit the flow of communication over the Internet. However, imposing the "knowingly" standard of fault in child sexual exploitation cases will eliminate the duty to monitor, and a plaintiff bringing this type of suit would need to prove, as an element of his or her claim, that the ISP knew about the child sexual exploitation.

3. Imposing the Proposed Liability Will Not Inundate the ISPs with Lawsuits

Imposing civil liability for knowingly receiving and/or distributing child sexual exploitation materials is also not likely to inhibit the growth of the Internet due to an increase in related litigation. Magistrate Judge Craven, in explaining her extension of § 230 immunity in *Doe v. Bates*, argued that "[i]f civil liability were possible, the incentive to bring a civil claim for the settlement value could be immense."[94] Professors Doug Lichtman and Eric Posner point out that a court makes a mistake "when it assumes that a mere accusation would be sufficient to trigger ISP

---

91. Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 at *4 (E.D. Tex. Dec. 27, 2006) (quoting *Zeran*, 129 F.3d at 333).

92. *See* Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 851 (W.D. Tex. 2007).

93. The plaintiffs in *Doe v. Bates* argued that "[i]t certainly is not impossible for Yahoo! to comply with federal laws prohibiting the knowing receipt and distribution of child pornography." Plaintiff's Objections, *Doe v. Bates*, *supra* note 89, at *9.

94. Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 at *22 (E.D. Tex. Dec. 27, 2006) (Craven, Mag. J., Report and Recommendation).

liability."[95] They explain that "[i]n a more familiar setting, that sounds absurd."[96] For example, they argue, it would be ludicrous to say that a court would really "hold a large bookseller accountable for defamation solely because a random patron informed the cashier that a particular title contained an unlawful communication."[97] If liability were imposed, ISPs would only be required not to knowingly allow the sexual exploitation of children on their Web sites, which would mean that "an ISP would not be required to do anything in cases where the only warning was an isolated accusation. . . ."[98] The requirement for citizens and other entities to comply with the law has not been lessened because of the threat of litigation. Similarly, in the context of child sexual exploitation, the threat of litigation should not allow ISPs to escape compliance with the law.

Additionally, ISPs are in a strong position to prevent the exploitation of minors on the Internet.[99] Professors Lichtman and Posner point out that § 230 specifically encourages ISPs to voluntarily address inappropriate action.[100] Section 230 immunizes ISPs from liability for "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."[101] Professors Lichtman and Posner note that the chain of liability often knows no bounds and they assert that, "as a practical matter the chain of liability cannot extend forever, and thus in the end choices must be made as to which entities are best positioned to support enforcement of the law."[102] Accordingly, the chain of liability should extend to ISPs in the case of knowingly allowing child sexual exploitation to occur on their sites because they are in a strong position to support enforcement of the law.

---

95. Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 252-53 (2006).

96. *Id.* at 253.

97. *Id.*

98. *Id.* at 252-53.

99. Professors Lichtman and Posner argue that ISPs "are in a good position to reduce the number and severity of bad acts online." *Id.* at 223. When faced with the growing problem of cyber-insecurity, they argue, "ISPs should be called into the service of the law." *Id.* at 224.

100. *Id.* at 224. Specifically, Lichtman and Posner argue that the language of § 230 itself supports the idea that ISPs are in a good position to reduce the number and severity of bad acts because the statute "encourages Internet service providers to address inappropriate content through voluntary private action." *Id.* at 223-24.

101. 47 U.S.C. § 230(c)(2)(A) (2000).

102. Lichtman & Posner, *supra* note 95, at 257.

D. Courts Should Not Extend § 230 Immunity to a Civil Claim Based on a Violation of § 2252A

1. The Exception to § 230 Immunity Provided by § 230(e)(1) and Title 18 U.S.C. § 2252A

Future courts should refuse to continue granting civil immunity to willful violators of a federal crime. ISPs such as Yahoo!, Google, and MySpace should not enjoy immunity under § 230 for civil claims arising out of Chapter 110 of Title 18 (relating to the sexual exploitation of children). Congress expressly stated in passing § 230(e) that § 230 immunity shall not affect Chapter 110 of Title 18, or any other federal criminal statute.[103] Title 18 U.S.C. § 2252A is plainly the type of statute imagined by Congress which would provide such an exception to § 230 immunity.

Section 2252A is a federal statute that makes it a crime to knowingly distribute child pornography.[104] It prohibits any person from knowingly receiving, shipping, transporting, distributing, or possessing, through any means of interstate commerce—*including by computer*—visual depictions of minors engaged in sexually explicit conduct.[105] It is a criminal offense[106] under § 2252A to have actual knowledge—such as repeated complaints that the service for which one is responsible is being used as the medium for consumption of child pornography—and then to do nothing about it.[107] Congress, in passing § 2252A, appears to have attempted to prevent the widespread transmission of child pornography over the Internet. Consequently, it is inconsistent with the expressed intent of Congress to bar civil actions and grant ISPs immunity when they are negligent to the point of committing a criminal offense by allowing this type of blatantly illegal material on their sites.

Section 230(e)(1) demonstrates that Congress intended that there be an exception to immunity in cases where ISPs knowingly allow the sexual exploitation of children on their sites. It follows that a civil claim based on an alleged violation of § 2252A should be recognized as falling within the exception for "enforcement" of a "federal criminal statute."[108]

---

103. 47 U.S.C. § 230(e)(1).

104. 18 U.S.C. § 2252A (2000).

105. § 2252A(a).

106. § 2252A(b). Section 2252A(f) also contains a provision for a private "civil remedy" for anyone aggrieved by a violation of the statute which further reveals Congress's intent to stop the widespread transmission of child pornography. § 2252A(f)

107. § 2252A(a)(2).

108. 47 U.S.C. § 230(e)(1).

2. Plaintiffs' Unsuccessful Attempt in *Doe v. Bates* to Bring a Civil Claim Under § 230 Based on an Alleged Violation of Title 18 U.S.C. § 2252A

The plaintiffs in *Doe v. Bates* proposed this approach and asserted that the exception under § 230(e)(1) should allow a civil suit to be brought based on alleged criminal acts.[109] They contended that their claim should not be barred by § 230 because they were seeking judgment under a provision of a criminal statute, § 2252A.[110] They argued that when Yahoo! decided to profit from its distribution of a Web site containing child pornography, it became a perpetrator as well.[111] To support their claim, the plaintiffs in *Doe v. Bates* provided an illustrative example of the seemingly prejudicial results of not recognizing such an exception to § 230 immunity under § 230(e)(1):

> Mr. Black, a hypothetical ordinary "user" of the Internet, can receive on his computer child pornography from his hypothetical friend Mr. Brown who took numerous illegal pictures of children. Mr. Black looks at the images (photos) and determines that they are indeed child pornography. Being an entrepreneur, Mr. Black decides to sell the photos over the Internet and not share any of the profits with Mr. Brown. Amazingly, he makes millions until the FBI stops the conduct. Mr. Black and Mr. Brown ultimately go to jail for a very long time for violating 18 U.S.C. § 2252A. Since 2252A also provides for civil remedies, the victims sue both Mr. Brown and Mr. Black. Though both are in jail, only Mr. Brown, the "content provider", can be liable in a civil action. Since Mr. Black is only a "user" of the Internet - not the content provider - he is immune from civil liability despite his reprehensible conduct.[112]

Doe v. Bates presented an issue of first impression to decide whether § 230 immunity should extend to a civil claim based on an alleged violation of § 2252A. Magistrate Judge Craven found that an intentional violation of criminal law is not an exception to immunity under § 230(e)(1) based on his finding that § 230(e)(1) only applies to criminal penalties of § 2252A.[113] She reasoned that § 230(e)(1) does not encompass civil claims because of the context of § 230(e)(1) and the common definitions of three terms: "criminal," "civil," and "enforcement."[114]

---

109. Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 at *20 (E.D. Tex. Dec. 27, 2006) (Craven, Mag. J., Report and Recommendation).

110. *See id.* at *3.

111. *See id.*

112. Plaintiff's Objections, *Doe v. Bates*, *supra* note 89, at *3-4.

113. Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 at *20-22 (E.D. Tex. Dec. 27, 2006) (Craven, Mag. J., Report and Recommendation).

114. *See id.* at *21.

Section 230(e)(1) states that all sections of Chapter 110 of Title 18[115] are to be "enforced."[116] Magistrate Judge Craven confined the meaning of "enforcement" to governmental actions. She says, "[i]n addition, Congress' use of the word 'enforcement' in Section 230(e)(1) again confirms that the exception refers to governmental action, not civil actions by a private litigant."[117] Magistrate Judge Craven provides the Black's Law Dictionary definition for "criminal"[118] and "civil"[119] but does not provide the definition for "enforce."[120] Black's Law Dictionary defines the term "enforce" as "[t]o give force or effect to (a law, etc.); to compel obedience to."[121] The definition is not limited in its construction to government enforcements.

Consistent with Magistrate Judge Craven's Report and Recommendation and Judge Folsom's ruling, ISPs can now be criminally prosecuted under § 2252A, but cannot be sued for civil remedies for that same conduct. Section 230(e)(1) should not be limited in its applicability to the criminal penalties of § 2252A. An alternative approach to interpreting the statute—i.e., interpreting it to apply to *all* enforcements, not just penal enforcements—would lead to a more logical result. Such a construction would be consistent with congressional intent and the plain language of the statute. From the standpoint of Congress, it makes little sense to subject ISPs to fines and prison sentences as a means of addressing child pornography, and then to say that "Congress nonetheless wanted to foster expansion of the Internet by protecting Internet service providers from attendant civil liability for their criminal conduct."[122] If Congress had intended to limit the meaning of § 230(e)(1), it could have used other language, such as "criminal enforcement" or "penal enforcement." Congress did not use such limiting language, and used instead, "[n]o effect on criminal law."[123]

---

115. Defined as "Sexual Exploitation and Other Abuse of Children," § 2252A falls within Chapter 110 of Title 18 of the U.S. Code.

116. 47 U.S.C. § 230(e)(1) (2000).

117. Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 at *21 (E.D. Tex. Dec. 27, 2006) (Craven, Mag. J., Report and Recommendation).

118. Black's Law Dictionary defines "criminal" as "[c]onnected with the administration of penal justice." BLACK'S LAW DICTIONARY 402 (8th ed. 2004).

119. Black's Law Dictionary defines "civil" as "[o]f or relating to private rights and remedies that are sought by action or suit, *as distinct from criminal proceedings*." BLACK'S LAW DICTIONARY 262 (8th ed. 2004) (emphasis added).

120. Doe v. Bates, No. 5:05-CV-91, 2006 WL 3813758 at *21 (E.D. Tex. Dec. 27, 2006) (Craven, Mag. J., Report and Recommendation).

121. BLACK'S LAW DICTIONARY 569 (8th ed. 2004).

122. Plaintiff's Objections, *Doe v. Bates*, *supra* note 89, at *16.

123. 47 U.S.C. § 230(e)(1) (2000).

In finding Yahoo! immune from civil liability, the court read 230(c)(1) broadly. It then proceeded to read the § 230(e)(1) exception to immunity narrowly. The result was an expansive interpretation that was not compelled by the language of the CDA, and that was incompatible with congressional intent and case law. If other courts continue[124] to follow this line of reasoning, then ISPs may further enjoy a far-reaching immunity that will allow the continued explosion of child pornography on the Internet.

IV. CONCLUSION

Minors are more susceptible to becoming victims of sexual predators on the Internet because of an overly expansive interpretation of § 230 immunity. In 2009, the continued expansion of the Internet remains an important goal, but such a goal does not require granting ISPs all-inclusive civil immunity from conduct that amounts to a violation of federal criminal law.

In order to curb the extension of § 230 immunity, several steps should be taken. Section 230 should be amended to reflect contemporary developments on the Internet and impose civil liability upon ISPs that knowingly allow the sexual exploitation of children on their sites. Future courts should recognize, in the meantime, that the policy and legal justifications proffered do not support extending CDA immunity to ISPs who knowingly permit the sexual exploitation of children on their Web sites. Any of the proposed courses of action will be a step in the right direction toward keeping minors safe on the Internet; however, "[n]o measure is a panacea."[125]

124. *See, e.g.*, Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007); Doe v. Sexsearch.com, 502 F.Supp.2d 719 (N.D. Ohio 2007).

125. Anne Barnard, *MySpace Agrees to Lead Fight to Stop Sex Predators*, N.Y. TIMES, Jan. 15, 2008, at B3 (quoting Connecticut Attorney General Richard Blumenthal).