Protecting Generation Z: A Brief Policy Argument Advocating Vicarious Liability for Internet Service Providers

By Mark G. Materna*

Introduction

IMAGINE YOU ARE SURFING THE INTERNET, perhaps looking for a last minute gift idea for a loved one. You have searched a number of e-groups[1] for ideas and stumble across a site called "Candyman." Thinking it may shed some light on your search, you enter the group and are soon shocked by the forum's dialogue. Rather than finding a medium with which to share innocent thoughts and content, you discover a forum aimed at posting, sharing, and transmitting illegal hard-core child pornography. Amidst this confusion, you also learn that the host site, Yahoo!, owns and profits from this e-group but is nevertheless immune from any liability whatsoever. Does this state of affairs concern you? Should it?

Unfortunately, given the current state of the law, such accounts are not reserved to conjecture or illusion. The aforementioned scenario mirrors the facts of *Doe v. Bates*,[2] a case indicative of how courts currently approach Internet Service Provider[3] ("ISP") liability for

* J.D., Pepperdine University School of Law and M.D.R., Straus Institute for Dispute Resolution, 2011; B.A., University of Pennsylvania, 2006. Special thanks to Dr. Babette Boliek, Associate Professor of Law at Pepperdine University School of Law, for her insight and guidance in preparing this article.

1. E-groups may be defined as "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." Katy Noeth, *The Never-Ending Limits of § 230: Extending ISP Immunity to the Sexual Exploitation of Children*, 61 Fed. Comm. L.J. 765, 770 n.35 (2009) (citation omitted).

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

3. An Internet Service Provider or "ISP" has been considered by courts to be an interactive computer service. Noeth, *supra* note 1, at 766 n.5. Section 230(f)(2) of the Communications Decency Act provides:

hosting content dealing with the sexual exploitation of children.[4] The outcome is an environment in which ISPs may host content that exploits children, including illegal hard-core child pornography, with virtually no liability. The current direction of the law in this context is unsatisfactory and requires reform. This article outlines the deficiencies in the current system and offers a fresh perspective aimed at ultimately making the Internet safer for the next generation.

Section I provides a background of § 230 of the Communications Decency Act ("CDA"), which governs immunity for providers and users of "interactive computer service[s]" that publish third-party content.[5] Section II summarizes some landmark decisions in § 230 jurisprudence and their shortcomings. In investigating a broad scope of alternatives, Section III outlines options for imposing liability for ISPs. Section IV introduces a policy argument advocating a voluntary vicarious liability program for ISPs while Section V addresses potential criticisms to this new program. Finally, to envision how this policy argument would translate to real-world application, Section VI applies the proposal to the facts of *Bates*.

I. Background of § 230 of the Communications Decency Act

A. Introduction to § 230

Section 230 of the CDA, enacted in 1996, provides immunity to ISPs by barring claims based on publication of third-party content.[6] An ISP is immune from state law claims if there is: "(1) [a] 'provider

> 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.

47 U.S.C. § 230(f)(2) (2000). Case law suggests an ISP is defined as a website that "functions as an intermediary by providing a forum for the exchange of information between third party users." Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 848 (W.D. Tex. 2007).

4. *See Bates*, 2006 WL 3813758, at *3; Noeth, *supra* note 1, at 770 (noting the judicial trend of broadening § 230 immunity). It is clear that the problem of child pornography still requires reform: "Some experts estimate that there are approximately 14 million pornographic websites with some posting approximately one million child abuse images." Beyond Borders, Inc., *What ISPs Could and Should Do to Prevent Child Sexual Exploitation*, http://www.beyondborders.org/wp/wp-content/uploads/2009/06/fact-sheet-ispsfinal2.pdf (last visited Oct. 20, 2011).

5. *See* § 230. As discussed, an ISP is considered an "interactive computer service" and, therefore, falls within the scope of the CDA. *See generally supra* note 3.

6. § 230(c)(1) ("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.").

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 ISP or other Defendant] 'as publisher or speaker' of that information."[7]

The scope of this provision extends to any "interactive computer service." Courts have interpreted this term broadly as including blogs, listservs, and forums as long as the information is provided to a third party.[8] Ultimately, § 230 may bar not only defamation-based claims but also claims relating to speech-based torts, misappropriation, invasion of privacy, and, most recently, claims of negligence against ISPs for failing to protect children from sexual predators.[9] In the context of ISPs, § 230 has generally provided immunity from both distributor and publisher liability.[10]

B. Narrow Exception to § 230

Despite the CDA's broad scope, Congress provided an exception to § 230. Subsection 230(e) states, in relevant part, that "[n]othing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, or any other Federal criminal statute."[11] As shall be discussed, courts have been unwilling to utilize this narrow exception. As a corollary, this exception is virtually useless in restricting broad liability for ISPs that are presently free to knowingly profit from hosting illegal child pornography.

---

7. Universal Comm. Sys. v. Lycos, Inc., 478 F.3d 413, 418 (1st Cir. 2007) (quoting 47 U.S.C. § 230(c)(1)). In addition, § 230(c) provides protection for "Good Samaritan" blocking and screening of offensive material. This provides protection 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." § 230(c)(2)(A). However, as shall be discussed, this standard is not a requirement for ISPs and is not clearly defined in relevant case law. *See generally infra* Part II.

8. Citizen Media Law Project, *Immunity for Online Publishers Under the Communications Decency Act*, http://www.citmedialaw.org/legal-guide/immunity-online-publishers-under-communications-decency-act (last visited Oct. 20, 2011). Generally, a listserv, or list server, is a program that automatically sends messages to multiple email addresses on a mailing list.

9. *See id.*

10. *See* Noeth, *supra* note 1, at 766.

11. § 230(e)(1). This section provides certain exceptions from civil liability including: (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 generally* § 230(e)(1)–(4).

C. Congressional Intent in Enacting § 230

Prior to enactment of the CDA, there was much confusion over distributor liability as it pertained to the Internet.[12] Most notably, Congress was prompted by two New York state court decisions that reached markedly different conclusions.[13]

In *Cubby, Inc. v. CompuServe*,[14] the court established a precedent for applying defamation law to the Internet medium. Plaintiffs brought an action for libel, unfair competition, and business disparagement based on allegedly defamatory statements made in a publication carried on the defendant's electronic bulletin board.[15]

Specifically, Cubby sued CompuServe, an ISP, over information contained in a CompuServe forum.[16] The forum was provided by an independent contractor without CompuServe's editorial participation.[17] In granting CompuServe's motion for summary judgment, the United States District Court for the Southern District of New York opined that CompuServe could not be liable because it did not know, nor did it have reason to know, about the alleged defamatory statements.[18] The court dismissed the case by finding that CompuServe should not be treated as a distributor even if it did not review content before it was hosted on its website.[19]

Only four years later, a similar issue was brought before a New York state court in *Stratton Oakmont Inc. v. Prodigy Services Co.*[20] In that case, Prodigy advertised itself as a "family oriented" computer network that used content guidelines and a software-screening program for its online bulletins.[21] The court found that, because of these measures, Prodigy was acting more like a "publisher" than a "distributor" and was thus fully liable for all the content hosted on its site.[22]

Cubby and *Stratton* illustrated an inconsistent and seemingly arbitrary court rationale. This resulted in a:

12. *See generally* Noeth, *supra* note 1.

13. *See* Sewali K. Patel, *Immunizing Internet Service Providers from Third-Party Internet Defamation Claims: How Far Should Courts Go?*, 55 VAND. L. REV. 647, 658–61 (2002).

14. 776 F. Supp. 135 (S.D.N.Y 1991).

15. *Id.* at 138.

16. *Id.* at 137–38.

17. *Id.*

18. *Id.* at 142.

19. 776 F. Supp. at 144.

20. 23 Media L. Rep. (BNA) 1794 (N.Y. Sup. Ct. 1995).

21. *Id.* at 1795.

22. *Id.* at 1798. In other words, the court opined that Prodigy was a publisher because it held editorial control over the Board Leader. *Id.*

> perverse upshot [where] . . . any effort by an online information provider to restrict or edit user-submitted content on its site faced a much higher risk of liability if it failed to eliminate all defamatory material than if it simply didn't try to control or edit the content of third parties at all.[23]

In response, Congress passed the CDA, which stated that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[24] While this was certainly a step forward in clarifying such jurisprudence, the Act contained "deceptively simple" language.[25] Ultimately, this language would cause more problems than it solved.

In passing this provision, Congress was most concerned with ensuring that the threat of litigation would not hinder the development of the Internet.[26] To guarantee this result, Congress attempted to protect online intermediaries from liability for unlawful third-party con-

23. Citizen Media Law Project, *supra* note 8.

24. 47 U.S.C. § 230(c)(1) (2000). *See generally* Matthew Schruers, *The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 213 (2002) ("Section 230 was originally intended to compete with the CDA. It was introduced as the Online Family Empowerment Amendment or the Cox/Wyden Amendment, and its dual purpose was to overrule *Stratton Oakmont* and to encourage private efforts to cope with Internet indecency." (footnote omitted)). It is also important to note that the CDA's enactment, at least in its original form, was short lived. A mere week after the statute was enacted, a Federal District court enjoined the operative provisions of the CDA. *See id.*; ACLU v. Reno, 24 Media L. Rep. 1379, 1381 (E.D. Pa. 1996) (granting temporary restraining order against enforcement of CDA); ACLU v. Reno, 929 F. Supp. 824, 883–84 (E.D. Pa. 1996) (preliminarily enjoining CDA provisions), *aff'd*, Reno v. ACLU, 521 U.S. 844 (1997) (United States Supreme Court upholding district court's opinion).

25. Citizen Media Law Project, *supra* note 8.

26. *See* § 230(b)(1), (2), (4). Congress also 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.

§ 230(a); *see generally* 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).

tent.[27] Also paramount to Congress's rationale in passing § 230 was that creating such immunity would subsequently remove disincentives for self-regulation of ISPs.[28] This rationale will be particularly relevant to revisit in discussing the tenets of a voluntary vicarious liability program for ISPs.

II. Section 230 Jurisprudence and its Shortcomings

A. The So-Called Seminal Case: *Zeran v. AOL*

In the scope of § 230 jurisprudence, *Zeran v. America Online, Inc.*[29] emerged as the ostensible seminal case; in reality, its rationale has been misapplied to cases that are factually distinguishable.[30] At issue in the case was a message anonymously posted on America Online's ("AOL") bulletin that advertised items glorifying the 1995 Oklahoma City bombing.[31] The contact information of Plaintiff Zeran was posted, though he had neither knowledge of nor involvement with the postings.[32] Zeran brought suit against AOL after they failed to remove the message, alleging 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 material."[33] In a landmark decision, the Fourth Circuit extended § 230 immunity to AOL, even though it had prior notice of the content's illegal nature.[34] In other words, given the set of facts, the court found that holding AOL liable

27. *See* Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758, at *3 (E.D. Tex. Dec. 27 2006) ("The Court finds that immunity from all private civil liability comports with the clear Congressional policies to avoid disincentives to innovation and to encourage self-regulation.").

28. *See* § 230(b)(4) ("It is the policy of the United States . . . (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 online material.").

29. 958 F. Supp. 1124 (E.D. Va. 1997), *aff'd*, 129 F.3d 327 (4th Cir. 1997).

30. *See id.*; 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). Though there has been some scholarly dialogue stating that *Zeran* was decided correctly, especially given the rise of Web 2.0, such commentary does little to address the unique aspect of child pornography. As such, these views mistakenly assert *Zeran* should be applicable in all cases involving § 230 immunity. *See* Cecilia Ziniti, *The Optimal Liability System for Online Service Providers: How* Zeran v. America Online *Got It Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583 (2008).

31. *Zeran*, 129 F.3d at 328.

32. *Id.*

33. *Id.* at 330.

34. *Id.* at 335.

for its exercise of a publisher's traditional editorial functions was barred by § 230.[35]

In retrospect, the Fourth Circuit's rationale in *Zeran* was sound. The court examined the particular facts of the case and found that the ISP should not be held accountable for content hosted on its website. However, this rationale has created a proverbial "slippery slope" where courts have inappropriately cited *Zeran* as precedent in extending § 230 immunity to facts that are entirely unrelated. As shall be discussed, most disconcerting is how the facts of *Zeran*—a case dealing with a bulletin advertising items glorifying the Oklahoma City bombing—have been applied to cases involving the sexual exploitation of children. Courts have not addressed how child exploitation cases may be different, and as a result, *Zeran* has remained the seminal case for § 230 immunity conflicts, regardless of whether such conflicts deal with the exploitation of children.

B. A Preview of Misapplication: *Aquino v. ElectriCiti, Inc.*

Even while the appeal in *Zeran* was pending, the district court's decision appeared to already be impacting other courts. In *Aquino v. ElectriCiti, Inc.*,[36] leaders of the "Temple of Set" religious group brought a claim against a California-based ISP called ElectriCiti over statements made by one of its subscribers.[37] Specifically, an ElectriCiti subscriber posted false statements on an anonymous online bulletin board alleging plaintiffs were involved in various illegal acts, including the satanic ritual abuse of children.[38]

Curiously, the California court did not address any differences between these facts and those in *Zeran*, even though they were markedly different. Instead, when ElectriCiti moved to dismiss the complaint, the court held that the case was preempted by § 230 of the CDA.[39]

35. *Id.* at 330. These traditional editorial functions include deciding whether to publish, withdraw, postpone, or alter content. *Id.*

36. 26 Media L. Rep. (BNA) 1032 (Cal. Super. Ct. 1997).

37. *Id.* Specifically, plaintiffs claimed that ElectriCiti negligently failed to ensure that its services were not used to assist a mentally unstable individual to continue his or her vendetta against other persons via the Internet. They also alleged that ElectriCiti actively assisted the third party subscriber in making the objectionable postings and that the subscriber was an agent and/or employee of ElectriCiti such that the actions were attributable to ElectriCiti.

38. *Id.*

39. *Id.*

Unfortunately, this would serve as a preview of the misapplication that other courts would employ when citing *Zeran* as authority to preempt claims under § 230, regardless of whether or not the case demonstrated drastic factual differences.

Not long after, when on appeal, *Zeran's* significance in the context of § 230 jurisprudence became more apparent. First, it evidenced that courts were, at the very least, aware of the idea of notice-liability and its potential shortcomings. Specifically, Judge Wilkinson "cited the potential effect of adopting *Zeran*'s arguments, noting the 'practical implications of notice liability in the interactive computer service context.' The sheer volume of notifications, he argued, would create a prohibitive, 'impossible burden.'"[40] Further, as previous scholarly discussion in this context had noted:

> The Zeran ruling changed the nature of scholarly discussion of ISP liability. Until Zeran, the debate had focused on the publisher/distributor distinction. This was essentially a debate over the standard of liability: whether a negligence regime was preferable to a strict liability regime. In Zeran, the Fourth Circuit discarded a liability regime in favor of a non-liability/conditional immunity regime. Following Zeran, the debate has turned on whether an immunity regime or a liability regime is appropriate.[41]

After *Zeran*, § 230 jurisprudence was at a critical juncture and would soon take a turn toward the nonsensical.

C. A Step in the Wrong Direction: *Doe v. Bates*

In *Bates*, an underage boy's photographs were posted on an illegal pornography e-group called "Candyman," which was hosted and operated by Yahoo![42] The group allowed members to exchange messages and provided a forum for posting, sharing, and transmitting "hard-core, illegal, child pornography."[43] Plaintiffs alleged Yahoo! knowingly hosted illegal child pornography and was liable for failing to prevent the content from being on its website.[44]

---

40. *See* Schruers, *supra* note 24, at 216–17 (citing *Zeran*, 129 F.3d at 333).

41. *Id.* at 217–19 (citing Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998)). In *Blumenthal*, Judge Paul Friedman opined that "[i]n some sort of tacit quid pro quo arrangement with the service provider community, Congress has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted." 992 F. Supp. at 52.

42. *See* Doe v. Bates, No. 5:05-CV-91-DF-CMC, 2006 WL 3813758, at *1 (E.D. Tex. Dec. 27, 2006).

43. *Id.* at *5 (citing Magistrate Judge Caroline Craven's Report and Recommendation); *see also* Noeth, *supra* note 1, at 770.

44. *Bates*, 2006 WL 3813758, at *3–4.

The Texas court, in applying § 230, had the opportunity to differentiate the facts from *Zeran* and recognize how child exploitation could possibly be approached differently because of its particularly vile nature and effect on minors. In making this argument, the court could have utilized the § 230(e) exception and made an argument that would have held Yahoo! liable to some extent. This exception existed at the time but still had yet to be utilized in the context of child exploitation. Instead the court relied on *Zeran* and found that § 230 immunity extended to Yahoo!, even if the ISP knowingly profited from an illegal website.[45] As a result, § 230 jurisprudence took a dangerous step toward allowing ISPs carte blanche to host any content they wish with virtually no liability. This ultimately provides more forums for those wishing to exchange illegal child pornography—a result that makes the Internet less safe for the next generation.

D. Aggrandizing the Problem: *Doe v. MySpace*

The rationale from *Bates,* which extended § 230 immunity for ISPs with regard to child exploitation, was soon extended beyond e-groups. In *Doe v. MySpace, Inc.*,[46] a thirteen-year-old girl created a profile on the networking site MySpace.[47] When she was fourteen, she was contacted via MySpace by Pete Solis, a nineteen year old.[48] After receiving her contact information and arranging a meeting, Solis sexually assaulted the minor.[49] The girl's parents brought suit against MySpace, alleging it should have taken some steps to protect minors on the networking site.[50]

The district court dismissed the case and granted MySpace § 230 immunity.[51] In making its decision, the court relied heavily on precedent from *Zeran* and *Bates* and found that because MySpace was sued in its capacity as a publisher, it was immune from liability.[52] Thus, the court aggrandized the problem; now § 230 immunity was applied to networking sites as well, and it appeared ISPs assumed virtually no liability for any content they hosted.

45. *Id.*
46. 474 F. Supp. 2d 843 (W.D. Tex. 2007).
47. *Id.* at 846.
48. *Id.*
49. *Id.*
50. *Id.* at 848.
51. *MySpace*, 474 F. Supp. 2d at 850–52.
52. *Id.* 848.

E. Expanding § 230 Immunity Even Further: *Doe v. SexSearch*

While *MySpace* expanded § 230 immunity to networking sites, it restricted such immunity to situations where the ISP was being sued in its capacity as a publisher. Shortly thereafter, however, this restriction was admonished in *Doe v. SexSearch.com*.[53] The controversy in *SexSearch* involved a plaintiff who alleged he had mistakenly engaged in intercourse with a minor who he met via the networking service SexSearch .com.[54] Pursuant to the rationale in *MySpace*, the Northern District Court of Appeals of Ohio did not evaluate the claim as pled but instead concentrated on Defendant's capacity as publisher and concluded that, since the claim rested on SexSearch's failure to remove the girl's profile or prevent her assaulter from communicating with her, the claims should be barred under § 230.[55] The court found the plaintiff was inappropriately attempting to "plead around" the CDA."[56] As a result, the court granted immunity to an ISP, even when it was sued in its general capacity as a host of content and not specifically in its capacity as a publisher.[57] Thus, the final restriction to immunity echoed in *MySpace* was breached, resulting in a system where ISPs are virtually never liable for the content they host.

In short, § 230 jurisprudence illustrates two significant shortcomings. First, it mistakenly relies on *Zeran*, a case addressing the distinguishable facts of a bulletin advertising items glorifying the Oklahoma City bombing, which is completely unrelated to child pornography or the exploitation of children. Although decided correctly given its particular facts, *Zeran* is not applicable to child exploitation cases. This discrepancy has not been addressed, yet courts continually use *Zeran* as precedent rather than examine the facts of each individual case as pled. Second, courts have been unwilling to use § 230(e) as a viable exception to cases dealing with the sexual exploitation of children. Instead, they have granted immunity to ISPs irrespective of whether they are sued in their capacity as publishers. These shortcomings have drastic consequences on the safety of the Internet for minors and require reform.[58]

53. 502 F. Supp. 2d 719 (N.D. Ohio 2007).

54. *Id.* at 722.

55. *Id.* at 727–28.

56. *Id.* at 727. The court held 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." Noeth, *supra* note 1, at 772.

57. *SexSearch*, 502 F. Supp. 2d at 728.

58. Child pornography is one of the fastest growing businesses online, and the content is becoming much worse. *See* INTERNET WATCH FOUNDATION, 2008 ANNUAL AND CHAR-

As the system presently stands, § 230 provides that civil liability may only be imposed on the individual posters of the content.[59] Thus, providers have no incentive to change their policies, as they are free to knowingly profit from hosting illegal material, even if it is as disturbing as hard-core child pornography. Boundaries of ISP protection under § 230 are far from satisfactory and have recently been found to extend beyond tort liability.[60] As a result, ISPs are being protected at the expense of children. A plethora of forums are available to transmit materials that sexually exploit minors. Instead of mitigating the avenues through which such content is available, the current system aggrandizes the problem by failing to regulate mediums through which such content can be exchanged, making it easier for sexual predators to exploit the next generation.

III. Options for Imposing Liability on ISPs

Having established that the present system is unsatisfactory, the next logical step in remedying the situation is an analysis of available options for imposing liability on ISPs. After analyzing four popular options, it becomes evident that a policy advocating vicarious liability is the most efficient and realistic.

ITY REPORT 7 (2009), *available at* http://www.iwf.org.uk/assets/media/IWF%20Annual%20Report%202008.pdf. In 2008, Internet Watch Foundation found 1,536 individual child abuse domains. *Id.* Of these domains, 58% were housed in the United States. *Id.* As of 2011, a total of 12,966 URLs contained child sexual abuse hosted on 1,595 domains worldwide. INTERNET WATCH FOUNDATION, 2011 ANNUAL AND CHARITY REPORT 12–14 (2012), *available at* http://www.iwf.org.uk/assets/media/annual-reports/annual%20med%20res.pdf. Also of concern is that 74% of the child victims appeared to be 10 years old or under while 64% of all the child sexual abuse URLs depicted sexual activity between adults and children, including the rape and sexual torture of the children. *Id.*

59. *See* § 230(c)(1).

60. *See, e.g.*, Gucci Am., Inc. v. Hall & Assocs., 135 F. Supp. 2d 409 (S.D.N.Y. 2001) (deny- ing § 230 immunity because the court ruled that, due to the plain language of § 230(e)(2), immunity did not apply to intellectual property claims); Kathleen R. v. City of Livermore, 104 Cal. Rptr. 2d 772, 781 (Ct. App. 2001) (finding that plaintiff's claims were preempted by § 230 when a child's parents sued the local public library after the child repeatedly downloaded sexually explicit images using the library computer); Stoner v. eBay Inc., 56 U.S.P.Q. 2d (BNA) 1852, 1855 (Cal. Super. Ct. 2000) (holding in dicta that, pursuant to *Zeran*, ISPs would not lose immunity unless they are "aiding and abetting" criminal activity); ''Schneider v. Amazon.com, Inc., 31 P.3d 37 (Wash. Ct. App. 2001) (opining that § 230 could protect against liability for breach of contract as well as website immunity).

A. No Liability

The first proposal, and the one most heavily favored by ISPs for obvious reasons, is a policy of no liability. No liability proposes that ISPs not be held responsible for any infringing activity, despite having actual or constructive knowledge of the infringement.[61] Given the aforementioned jurisprudence, one might argue the current system practices no liability for ISPs, despite the exception in § 230(e). Such a proposal advocates a system where:

> [n]on-regulation of the Internet could be considered a controversial approach to Internet regulation. However, in light of the failed efforts to impose any coherent control over information available on the Internet, it is better to allow the Internet to develop and evolve before hastily intervening. When the Internet's growth has slowed and the effects of Internet use are plain, only then can the law hope to create a proper regulatory regime. For now, the governments of the world should allow the Internet to develop, grow, expand, and realize its full potential.[62]

A system based on no liability or non-regulation for ISPs would have one positive result: it would be in line with congressional intent by ensuring the threat of litigation would not hinder the development of the Internet.[63] After all, if it is uniformly recognized that ISPs are not responsible for the content they host whatsoever, parties would be precluded from bringing frivolous claims against ISPs. At the same time, this would further promulgate an unsafe environment for children on the Internet. The current system, at least in theory, holds ISPs somewhat responsible for the content they host. Despite this potential for liability, this system has nevertheless resulted in an unsafe Internet environment where many avenues such as e-groups and networking sites may be used to sexually exploit children. A system without liability, even just in theory, would only serve to make matters worse and would be a step away from regulating such avenues. A system based on no liability for ISPs, therefore, is insufficient.

B. Strict Liability

Strict liability offers the most stringent form of liability but is relatively unrealistic in practice. Such a system advocates ISPs be held re-

61. *See* Nassir Ayyaz, *Liability of ISPS for Content Hosted by Them*, SMASHITS.COM, http://articles.smashits.com/articles/legal/110303/liability-of-isps-for-content-hosted-by-them.html (last visited Oct. 21, 2011).

62. Shamoil Shipchandler, *The Wild Wide Web: Non-Regulation as the Answer to the Regulatory Question*, 33 CORNELL INT'L L.J. 435, 458 (2000) (footnote omitted).

63. *See* 47 U.S.C. § 230(b)(1), (2), (4) (2000).

sponsible for all the material they host regardless of their level of knowledge.[64] Since ISPs would be accountable for the services they provide, like all other big publishers and distributors, they would have a responsibility to review all the material hosted by them.[65]

Though this would undoubtedly have a dramatic impact on reducing illegal material that sexually exploits children, in practice such a system is highly impractical.[66] ISPs are quite different from distribution companies because they deal with a unique medium—an electronic environment.[67] Such an environment is ever-changing, and it would be neither possible nor economically viable for an ISP to undertake such responsibility.[68]

In particular, because of the sheer volume of Internet content, filtering can only be done with automated tools.[69] Even if implemented, such filtering techniques "yield many false positives and sometimes are over-inclusive."[70] Secondly, the filtering process entails high costs for staff and equipment. This may have a pernicious effect where these costs are passed on to the Internet-users.[71] Ultimately, "[g]iven its high cost, filtering may strike at the heart of the internet. Large scale filtering has a reductive effect on the internet industry . . . at the expense of innovation of the internet."[72] Since it puts far too much responsibility on ISPs, strict liability is not a viable option.

C. With-Fault Liability

A third option to consider is with-fault liability, which, though not as stringent as strict liability, ultimately results in the same shortcomings. A cornerstone tenet of with-fault liability is that the ISP had actual or constructive knowledge of the infringing material hosted.[73] In

64. Ayyaz, *supra* note 61; *see also* Jonina S. Larusdottir, *Liability of Intermediaries for Copyright Infringement in the Case of Hosting on the Internet*, 47 SCANDINAVIAN STUD. L. 471, 474 (2004).

65. Larusdottir, *supra* note 64, at 474–75.

66. *See generally* Schruers, *supra* note 24, at 249 (asserting that shortcomings of strict liability in this context exist because such liability fosters a self-interested "Dennis calculus" which corrupts the efficiency of a negligence regime).

67. *See* Ayyaz, *supra* note 61.

68. *Id.*

69. Maurice Schellekens, *Liability of Internet Intermediaries: A Slippery Slope?*, 8 SCRIPTED J. L., TECH. & SOC'Y, 154, 169 (2011), *available at* http://www.law.ed.ac.uk/ahrc/script-ed/.

70. *Id.* at 167.

71. *Id.* at 168–69.

72. *Id.* at 169.

73. *See* Anjali Anchayil & Arun Mattamana, *Intermediary Liability and Child Pornography: A Comparative Analysis*, 5 J. INT'L COM. L. & TECH. 48 (2010).

cases where there was no actual knowledge, the ISP would be presumed to have constructive knowledge and be held liable.[74]

Like those who support a strict liability regime, proponents of with-fault liability would likely note that such a system would place much more responsibility on ISPs to monitor material they host, which in turn will make it more difficult to transmit materials that sexually exploit children.[75] Though this supposition is undoubtedly true, this argument is countered by ISPs who feel there should be a standard where the ISP is required to have actual knowledge of the content hosted.[76] Without such a standard, the policy is virtually identical to strict liability—as discussed, it proposes unrealistic standards with little or no pay-off for the ISP.[77] Accordingly, such an option is not viable and should be dismissed.

D. Vicarious Liability

A final option to consider in formulating a framework under which ISPs may be held accountable is vicarious liability. This type of liability would be imposed on an ISP where it has the right and ability to supervise the infringing activity from which it derives direct financial gain.[78] Such liability would arguably make ISPs more accountable for the content they host. As a corollary, ISPs will be more discerning about the type of content hosted.[79] The hope is that such a system would limit the mediums through which illegal child pornography is readily available.

Despite these potential positive aspects, there are two hurdles that generally prevent vicarious liability from being imposed on ISPs.[80] First, vicarious liability requires that there be some employer-servant relationship between subscribers and ISPs.[81] Second, ISPs must directly benefit from the content uploaded by subscribers.[82] Since ISPs typically only host content and are not directly benefitted

74. *See* Ayyaz, *supra* note 61.

75. *See generally id.* (recognizing such an argument in support of a strict liability regime).

76. *Id.*

77. Since the economic makeup of with-fault liability parallels strict liability, the economic shortcomings are also applicable. *See generally* Schruers, *supra* note 24.

78. *See* Ayyaz, *supra* note 61.

79. *Id.*

80. *Id. See generally* Craig A. Grossman, Sony *to* Grokster, *The Failure of the Copyright Doctrines of Contributory Infringement and Vicarious Liability to Resolve the War Between Content and Destructive Technologies*, 53 BUFF. L. REV. 141 (2005).

81. *See* Ayyaz, *supra* note 61.

82. *Id.*

from their subscribers, vicarious liability does not appear to be a viable option at first glance.

Interestingly, however, an exception to these requirements exists in the rare circumstances when an ISP owns the particular website where the content is hosted.[83] In such scenarios, the ISP receives direct financial gain from use of the website, which in turn constitutes an employer-servant relationship. Given this exception, vicarious liability is a viable option in such circumstances and seems a workable first step toward a program that can make the Internet safer for the next generation.

IV. Policy Argument for Vicarious Liability

Once vicarious liability has been established as a cornerstone to a proposal, a policy argument aimed at remedying the present deficiencies of § 230 should be discussed. This section will address the scope of this proposal, the role the Federal Communications Commission ("FCC") must play in this context, and the perspective through which this proposal should be viewed.

A. Scope of the Program

In the interest of promoting a relatively conservative approach that does not drastically disrupt current legal precedent, the scope of the program should pertain only to situations where the ISP owns the website where the illegal material is being shared, posted, or transmitted. Moreover, the program only relates to illegal material—in this case, child pornography—which is offered no constitutional protection.[84] Finally, the program will be entirely voluntary; that is, ISPs will opt into undertaking vicarious liability for the content they host. The incentive for doing so is getting a "seal of approval" from the FCC, which communicates to parents that the particular ISP is safer for their children. With such a perception, parents will be more willing to allow their children to use such programs. As more ISPs enroll in the

83. *Id.*

84. Child pornography that uses actual children is illegal and offered no constitutional protection. *See* 18 U.S.C. § 2251 (2006). Child pornography that is "obscene" is illegal regardless of whether it uses children. *See* 18 U.S.C. § 1462 (2006). While ISPs that become aware of child pornography must report this information to the National Center for Missing and Exploited Children, there is no duty to monitor sites for such content. *See* 18 U.S.C. § 2258A (Supp. II Vol. 2 2008); Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 227 (2008) (asserting the conflict between speech and victim compensation as a result of § 230 is illusory in the first place).

program, those outside the scope of the FCC "seal of approval" will find it in their best interests to take part in this effort, if only as a mechanism to compete with their business opponents.

The effect of this narrowly tailored program will bypass the hurdles associated with vicarious liability. First, the ISP is directly benefitted from the content since it owns the particular website where the illegal content is hosted. Second, this creates an employer-servant relationship where the ISP benefits from the traffic provided by subscribers—the employers.[85] Thus, by advocating a narrow scope, this policy argument illustrates a workable first step where vicarious liability is a viable option.

B. The Role of the FCC

For this program to be a workable solution, FCC involvement is of paramount importance. As alluded to previously, this program advocates that ISPs voluntarily opt-in so as to preclude a backlash from ISPs who may feel the FCC is cracking down on their roles as service providers. Rather than propose drastic measures, the FCC would first grant programs the "seal of approval" discussed earlier.

In addition to an FCC "seal of approval," this program also requires there be immunity for ISPs who undertake liability. While there is no default duty to monitor content, should an ISP become aware of content violations on hosted websites, it has a duty to report them.[86] Failure to adhere to these principles can result in fines up to $150,000 for a first offense and up to $300,000 for a secondary offense.[87] By granting participating ISPs immunity from such provisions and allowing them to self-regulate and take on vicarious liability, there will be more of an incentive to enroll in the proposed program.

85. *See* Ayyaz, *supra* note 61.

86. Notably:

> Whoever, while engaged in providing an electronic communication service or a remote computing service to the public through a facility or means of interstate or foreign commerce, obtains actual knowledge of any facts or circumstances described in paragraph (2) shall, as soon as reasonably possible—(A) provide to the CyberTipline of the National Center for Missing and Exploited Children, or any successor to the CyberTipline operated by such center, the mailing address, telephone number, facsimile number, electronic mail address of, and individual point of contact for, such electronic communication service provider or remote computing service provider; and (B) make a report of such facts or circumstances to the CyberTipline, or any successor to the CyberTipline operated by such center.

18 U.S.C. § 2258A(a)(1)(A)–(B).

87. § 2258A(e).

C. Sui Generis Perspective

As a final aspect to this program, a sui generis perspective[88] should be adopted because this material pertains specifically to illegal child pornography. ISP vicarious liability should be addressed on its own and not lumped into irrelevant case law such as *Zeran*. Behind this perspective is the logical premise that regulation of child pornography illustrates a unique concern for the well-being of minors and their exploitation via the Internet.

Such a rationale, first and foremost, fosters a mindset where the exceptions under § 230(e) are considered by courts as realistic options against granting carte blanche immunity to ISPs. In doing so, this important exception will regain its teeth as a mechanism in protecting children in the context of child exploitation via the Internet.

Furthermore, a sui generis perspective will allow members of the legal community, most notably judges, the opportunity to recognize the differences between child exploitation cases and other irrelevant case law. Most importantly, this will minimize courts' reliance on *Zeran,* which, as previously established, may illustrate a sound decision but is not relevant in the context of cases involving child exploitation. In taking this important step, courts can move toward examining cases as pled in an effort to establish more relevant common law in this context.

D. Policy Argument and Congressional Intent

Taken in the aggregate, the policy argument will also be in line with the congressional intent behind § 230 of ensuring that the threat of litigation would not hinder the development of the Internet.[89] Additionally, Congress hoped that creating such immunity would subsequently remove disincentives for self-regulation by ISPs.[90]

In addressing the threat of litigation, the proposed policy would not only preclude an increase but would actually ensure a decrease in litigation. Since ISPs enrolled in the program would hold a "seal of approval" from the FCC, they would already be in compliance with relevant regulations, at least in regard to websites they themselves own. Therefore, it would be highly unlikely that such ISPs would be in situations where their websites are acting as forums for hosting illegal

88. Sui generis literally means "of its own kind" and is used to describe something that is unique or different. BLACK'S LAW DICTIONARY 126 (9th ed. 2009).

89. *See* 47 U.S.C. § 230(b)(1), (2), (4) (2000).

90. *See* § 230(a).

hard-core child pornography. As such, frivolous litigation would be curbed, which would also conform to congressional intent.

In addition to the threat of litigation, Congress also reasoned that, in the absence of § 230 immunity, there would be a disincentive for ISPs to regulate themselves.[91] The proposed policy argument precludes such a result and is consequently in line with the legislative intent. In fact, the proposed argument is structured so that there is an incentive for ISPs to regulate themselves.

E. Summary of Benefits

In sum, the program would manifest a number of benefits. First and foremost, the proposed policy will allow ISP-owned websites to be more closely regulated. Consequently, some of the content hosted on these websites, namely content involving illegal, hard-core child pornography, will be virtually nonexistent in such forums. At the same time, since the scope of this program is relatively narrow, the burden on ISPs would be minute.

In addition, the policy will create incentives for parents to subscribe to better-regulated ISPs; after all, parents will be more willing to subscribe to ISPs that are safer, better regulated, and backed by the FCC. An increase in subscription from such parents will carry with it the added benefit of offsetting any financial burdens enrolled ISPs may incur as a result of the self-regulation. Thus, there will be a mutual benefit: parents and society will benefit from better-regulated ISP-owned websites while the ISPs will likely receive an increase in business as a result of the FCC "seal of approval."

V. Addressing Potential Criticisms

Like any new policy argument, this proposal is likely to be met with criticism. In preemptively addressing foreseeable criticisms, the policy argument's practicality becomes that much stronger. Potential criticisms would likely concentrate on three categories: cost, technology, and social implications.

A. Cost

Undoubtedly, the cost of regulating a high volume of content on a website is high. The cost of merely regulating ISP-owned websites,

91. *See* § 230(b)(4).

however, would not be nearly as daunting.[92] In addressing this concern, it is important to note that this policy argument proposes that ISPs would only be regulating those websites that they own. Moreover, immunity from FCC regulations, coupled with increased business from an FCC "seal of approval," will likely generate enough income for ISPs to balance any outstanding costs. In sum, the policy argument presents a viable solution that would likely not be financially detrimental to participating ISPs.

ISPs with deep pockets could present another problem in this context, in that would-be child pornographers might "forum shop" for jurisdictions in which affluent ISPs are headquartered in order to avoid individual liability. While this criticism has already been waged by other commentary it still recognizes that, despite this potential shortcoming, vicarious liability still presents the most obvious option:

> [F]rom a policy perspective, holding corporations vicariously liable for the actions of private individuals seems inappropriate when it will not have any significant impact on those who upload objectionable content to the Internet. Individuals need only shop in a favorable jurisdiction for ISPs with deep pockets. Unfortunately, despite the inherent difficulties with regulating the Internet through private corporations, it is the most likely course of action.[93]

B. Technology

Another foreseeable criticism of the proposed policy argument centers on technological shortcomings. Current technology has not yet reached the level where it can be viably administered to regulate the Internet: "ISPs are not yet equipped with the requisite technology to avoid the violations over the Internet. This requires high-tech language and image processing and surely the technology is so far not that advanced to cope with the problem of embedding technological measures in the servers of ISPs."[94]

This argument, however, is based on the assumption that the regulation would be broad in scope and encompass all content hosted by the ISP. Much like the cost-based criticism addressed above, the technological aspect of the proposal is viable, because it requires the ISP only deal with a relatively narrow portion of ISP-hosted content: con-

92. *See* Anchayil & Mattamana, *supra* note 73, at 48 (asserting "[i]ntermediaries seemed a viable option as they have the ability to regulate the content online at very minimal costs").

93. *See* Shipchandler, *supra* note 62, at 456.

94. *See* Ayyaz, *supra* note 61.

tent owned by the ISP. When understood through this narrow scope, the need for high-tech language and image processing becomes much less necessary. Similar technological measures have already been instituted with positive results on a wider scale than that proposed by this policy argument. Since 2004, British Telecom has used a system called "Cleanfeed" that restricts access to child pornography sites from its 2.7 million Internet subscribers.[95] The system filters specific domain names or unique numeric addresses associated with the web server hosting the site.[96] The lists are then supplied and updated by an industry-monitoring group named the Internet Watch Foundation.[97] Other measures have also been instituted including restricting underage users of mobile devices from accessing adult content, moderating chat rooms and other interactive services in which children are likely to participate, and generally making sure that child protection mechanisms keep pace with technological advancements.[98] While such proposals create a risk of infringing freedom of expression, the risk is outweighed by the dramatic effect such measures could have on protecting children.[99]

C. Social Aspects

A final potential criticism to consider is how society will view a system where ISPs regulate the content they host and the impact this would have on regulating the Internet as a whole. By granting an ISP the responsibility of regulating websites where they host content, there is a concern that the ISP will have too much power to regulate

95. *See* Beyond Borders, Inc., *supra* note 4.

96. *Id.* It is important to note that, to date, British Telecom has not made any plans to expand the project beyond child pornography sites. There has also been a backlash from sites that believe they were wrongfully blocked. *Id.*

97. *Id.*

98. *Id.*

> The UK Home Office recommends that public interactive communication providers undertake a risk assessment of the potential their service has to harm children. If there is a risk to children, then they should employ moderation, which involves a person or technical filter being responsible for reviewing content posted by users. Technical moderation attempts to filter words and phrases it has been programmed to identify, and telephone and e-mail addresses. However, it can be outwitted by the creative use of combinations of numbers, letters and punctuation marks. Human moderation is more effective and can be employed in a variety of ways; content can be reviewed before it becomes visible to other users, after it becomes visible, a sample of content can be reviewed, or moderation can take place only after a request for intervention is made.

Id. (citation omitted).

99. *Id.*

content on the Internet.[100] In a broad context, there is apprehension that ISPs under the proposed program would have the power to regulate content on the Internet as they see fit.[101] Such a result would be in conflict with a major purpose of the Internet, which is to foster the free flow of ideas.

To counter this argument, one need only examine the scope of the proposed policy. ISPs that choose to participate in the program will be vicariously liable for, and thus would regulate, only content on websites they own. Since many ISP web-hosting services include rate restrictions that limit traffic volume, they are typically more popular for smaller personal sites with low amounts of traffic and not conducive to businesses or forums that generate large amounts of traffic.[102] Accordingly, the program's overall negative effect on the free flow of information over the Internet would be nominal. Such an infinitesimal effect on the free flow of information is a small price to pay for a measure that will prevent the dissemination of content that exploits children.

VI. Real World Application: *Doe v. Bates*

In order to grasp how the proposed policy argument would relate to real-world application, it will be examined in the context of *Bates*. Had Yahoo! voluntarily enrolled in the proposed program, it would have undertaken vicarious liability for the content shared, posted, or transmitted on the websites that it owned. Since the scope of Yahoo!-owned websites would be relatively narrow in relation to the scope of the Internet as a whole, the cost of regulating such sites would not have had a dramatic impact on the free flow of information over the Internet. In return for assuming vicarious liability under the program, Yahoo! would not only receive an FCC "seal of approval" that would likely draw more parents to use it as an ISP, but it would also receive immunity from certain FCC regulations that could be potentially costly.[103]

Applying the program to the facts of the case, Yahoo! would have been monitoring the "Candyman" e-group in a cost-efficient manner and would have likely recognized the posting of illegal hard-core child

100. *See id.*

101. *See id.*

102. Jennifer Kyrnin, *Before You Choose a Web Hosting Service*, ABOUT.COM, http://webdesign.about.com/od/webhosting/bb/aabhosting.htm (last visited June 26, 2012).

103. *See generally* 18 U.S.C. § 2258A (Supp. II Vol. 2 2008) (outlining the scope of potential fines for not adhering to current FCC regulations in this context).

pornography on an e-group which it owned. A technological system such as "Cleanfeed" would filter specific domain names or unique numeric addresses associated with the web server hosting the site. As a result, those seeking to exploit children over the Internet would be unable to candidly post illicit content in mainstream forums. In turn, people randomly surfing the Internet, including children, would be less likely to stumble across such disturbing material. The success of the program would be twofold: (1) it would take a step toward a better-regulated Internet in the interest of children while also fostering an atmosphere for friendly competition among ISPs; and (2) it would help courts recognize the sui generis nature of child exploitation cases so that new precedent could be adopted in place of *Zeran*. Such a result would be in line with the congressional intent behind § 230 and would take a small step toward making the Internet safer for the next generation.

Conclusion

The state of the law regarding ISP liability for hosting content dealing with the sexual exploitation of children is unsatisfactory. Section 230 of the CDA provides civil immunity for ISPs from state law claims. In the context of hosting content that illegally exploits children, ISPs have been granted immunity from virtually any content they host.

Section 230 jurisprudence illustrates two important shortcomings. First, it mistakenly relies on *Zeran*—a case that hinged on a factual analysis entirely different from cases involving sexual exploitation of children. Rather than address this phenomenon, courts have used *Zeran* as a precedent in granting § 230 immunity. Second, courts have been unwilling to use § 230(e) as an exception in cases—such as those involving child exploitation—where ISP immunity may be inappropriate.

After analyzing a number of options for imposing liability on ISPs, it becomes evident that only a policy argument advocating vicarious liability is viable. Such a program would be voluntary in an attempt to be conservative in its approach. The scope of the proposed policy would only be applicable to circumstances where the ISP owns the website on which the content is hosted. In doing so, the program would bypass two common hurdles to typical vicarious liability proposals: the existence of an employer-servant relationship and the direct benefit to the ISP.

Moreover, the program would utilize FCC participation by granting immunity to participating ISPs from certain regulations and would also give a "seal of approval" that would serve to increase business to participants. In a broad context, a sui generis perspective should be used to differentiate other cases from cases that involve the particularly vile nature of child exploitation. Ultimately, this proposal is in line with congressional intent as it would not hinder the wider development of the Internet and would create incentives for ISPs to regulate themselves.

After dismissing a number of potential criticisms to the proposed policy argument, it becomes evident that this proposal is a viable first step toward remedying the current situation. Undoubtedly, the process toward making the Internet significantly safer for the next generation will be arduous and time-consuming. This proposal is a first step in the right direction. The hope is that, though policy arguments cannot realistically prevent situations such as the one in *Bates* overnight, this policy can provide a basis toward precluding similar results in the future.