2007

Regulating Cyberbullies Through Notice-Based Liability

Bradley A. Areheart

THE YALE LAW JOURNAL POCKET PART

BRADLEY A. AREHEART

Regulating Cyberbullies Through Notice-Based Liability

With the growth of the Internet's uses and abuses, Internet harassment is making headlines.[1] Given its immediacy, anonymity, and accessibility, the Internet offers an unprecedented forum for defamation and harassment. The salient problem with such "cyberbullying" is that victims are typically left without adequate recourse. The government should provide recourse by curtailing the near absolute immunity Internet Service Providers (ISPs) currently enjoy under the Communications Decency Act (CDA)[2] and implementing a notice and take-down scheme—similar to that for copyright infringement under the Digital Millennium Copyright Act (DMCA)[3]—for certain torts.

I. PRESENT OPTIONS AVAILABLE TO VICTIMS OF CYBERBULLYING

A victim of cyberbullying generally has two options for responding to Internet harassment, both of which lack any meaningful likelihood of success.

1. *See, e.g.*, Ellen Nakashima, *Harsh Words Die Hard on the Web*, WASH. POST, Mar. 7, 2007, at A1; Alex Pham, *Cyber-bullies' Abuse, Threats Hurl Fear into the Blogosphere*, L.A. TIMES, Mar. 31, 2007, at C1.
2. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified in scattered sections of 18 and 47 U.S.C.).
3. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified in scattered sections of 17 U.S.C.).

First, the person may pursue a legal remedy against the individual most directly responsible for inflicting the harm under one or more tortious causes of action. User anonymity, however, often makes it impossible to identify the harasser. Even if that hurdle can be overcome, legal action is costly, and the bully may well be judgment-proof.

The victim's second option is to employ extralegal means to confront the harassment. This might include attempting to respond personally; recent anecdotal evidence, however, suggests this may only make matters worse.[4] Alternatively, the victim could hire a company that specializes in destroying damaging online content or having it removed.[5] However, the success of such a company depends on the cooperation of ISPs, since a provider has no duty to remove such content, even if it is tortious. This quandary is exacerbated by the increasing number of providers who disclaim any responsibility for content and, instead, purport to be neutral forums for information and discussion.

The CDA effectively immunizes ISPs from tort liability. The CDA was passed in 1996 to regulate pornographic material on the Internet, but Section 230 added sweeping protection for Internet companies, directing, "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."[6] Courts have interpreted Section 230 broadly. For example, the Ninth Circuit held that the moderator of a listserv who posted an allegedly defamatory email authored by a third party was entitled to CDA immunity.[7] Another court refused to strip immunity under the CDA even though the ISP had an active role in producing the online content that was the basis for the suit.[8] The Fourth Circuit has interpreted the CDA to immunize providers even when they have notice that the content is tortious.[9]

Accordingly, victims currently lack meaningful redress, but modestly reforming ISP immunity could give them effective options.

---

4. *See* Nakashima, *supra* note 1 (noting that one victim's efforts to defend herself were rebuffed online by an anonymous poster's comment, "If we want to objectify, criticize and [expletive] on [expletive] like her, we should be able to.").

5. *See, e.g.*, ReputationDefender, http://reputationdefender.com/campaign_home.php (last visited Aug. 22, 2007).

6. 47 U.S.C. § 230(c)(1) (2000).

7. Batzel v. Smith, 333 F.3d 1018, 1030 (9th Cir. 2003).

8. *See* Blumenthal v. Drudge, 992 F. Supp. 44, 51-53 (D.D.C. 1998) (holding AOL had immunity for defamation liability, even though it had a contract with Matt Drudge that paid him to produce content).

9. Zeran v. America Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997) (holding that even notice of the content cannot serve as a basis for liability).

II. STRIPPING ISP IMMUNITY FOR CERTAIN CYBERWRONGS

It is sensible for ISPs to bear some responsibility for cyberwrongs. Third-party liability is traditionally warranted where one of two factors is at work: (1) a party is in a good position to redress another's bad acts through some sort of "control"; or (2) a party is able to account for and pass on the costs associated with liability and thus influence the "activity-level."[10] One or both of these factors are present for most ISPs. Under the DMCA, ISPs are understood to encompass suppliers of conduit services, which include Internet access, chat rooms, and web hosting services.[11] Accordingly, under the first factor, most ISPs operate as gatekeepers of some sort and thus have some degree of control over cyberbullying. For example, ISPs may disable Internet access to violative content, remove tortious material, or even terminate the account of a cybertort recidivist. Under the second factor, any ISP that charges for its services is able to account for negative externalities associated with its service and pass them on through the cost of subscription, affecting the activity-level. Although immunity under the CDA may have been warranted in 1996 when the Internet was a fledgling industry and Congress was reticent to take any action that would limit its growth,[12] this concern is now less compelling. Accordingly, ISPs are a logical entity to bear the costs of indirect liability.

The government should implement a notice and take-down regulatory scheme, similar to that under the DMCA, to curtail ISP immunity for certain forms of tortious cyberbullying.[13] Under the DMCA, ISPs generally have immunity when they act as mere conduits for material.[14] However, where an ISP provides system caching, information storage, or information location tools, and it receives actual notice of the infringing material, it must remove the content or risk liability through the loss of immunity.[15] The DMCA provides that an ISP has not received sufficient notice where the information provided does not furnish a sufficient basis for the ISP to determine if the content

10. Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 S. CT. ECON. REV. 221, 230-33 (2006).

11. 17 U.S.C. § 512(k)(1)(A) (2000); *In re* Verizon Internet Serv., 257 F. Supp. 2d 244, 269 n.26 (D.D.C. 2003); *see also* Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 254-56 (2005) (explaining the various roles an ISP may play as an "internet intermediary").

12. One of the clearly stated policy goals for Section 230 was "to promote the continued development of the Internet." 47 U.S.C. § 230(b)(1) (2000).

13. *See generally* Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 389-410 (2005) (proposing a similar—albeit much broader—notice regime).

14. 17 U.S.C. § 512(a) (2000).

15. § 512(b)-(d).

infringes upon a copyright.[16] If the ISP decides to remove the material, a counternotice procedure allows an alleged infringing user to challenge the take-down in federal district court and have her content "put back" on the Internet.[17] The ISP may then either put back the material and retain immunity or refuse to replace the material and subject itself to possible liability. Additionally, the DMCA provides a general right of action to pursue damages for take-down or put-back requests that are made in bad faith.[18] Using these DMCA procedures as a model, a similar regime within the CDA would require ISPs to remove tortious content upon adequate notice from the victim or waive immunity.

Though some scholars have proposed a notice and take-down solution modeled after the DMCA, their proposals are too sweeping to permit reasonable analogy with the DMCA's notice provisions for copyright infringement. One proposal would extend notice liability to any civil or criminal claim, including all claims sounding in tort.[19] However, one implicit rationale behind a notice and take-down scheme for alleged copyright infractions is that infringement claims are at least somewhat susceptible to investigation and judgment by the ISP. In contrast, to permit notice liability for *all* torts would require companies to make decisions about torts that are notoriously ambiguous, such as negligence and intentional infliction of emotional distress. Imposing notice liability on ISPs for such torts might induce them to over-comply with notice and take-down requests simply to avoid potential liability. Accordingly, any reform must be carefully tailored to survive legal and logical criticism on both workability and free speech grounds.

III. ADDRESSING OBJECTIONS ON FIRST AMENDMENT AND WORKABILITY GROUNDS

In any discussion of how to regulate the Internet, the elephant in the room is the First Amendment, which protects a considerable portion of cyberbullying as various forms of opinion speech.[20] Some of the most extreme examples of Internet harassment are tortious and thus not protected by the First

16. *See* § 512(c)(3).

17. § 512(f)-(g).

18. § 512(f).

19. *See* Rustad & Koenig, *supra* note 13, at 389 ("We favor a synchronized 'notice, takedown, and put-back' regime for *all civil and criminal wrongdoing*.") (emphasis added).

20. *See* Eugene Volokh, *Speech as Conduct: Generally Applicable Laws, Illegal Courses of Conduct, "Situation-Altering Utterances," and the Uncharted Zones*, 90 CORNELL L. REV. 1277, 1304 (2005) ("Under nearly every theory of free speech, the right to free speech [must] generally include in considerable measure the right to offend people . . . .").

Amendment. Still, serious questions remain. For example, how can the government regulate unprotected forms of speech without chilling or inflicting collateral damage on protected expressions?[21] Regulating speech through private companies admittedly presents unique dangers that are not encountered by regulating end users. For example, companies have an incentive to steer clear of liability by regulating more content than is needed, since the value of retaining any one customer is marginal.[22] Additionally, private abuses of discretion are likely to be less visible than public sanction of free speech.[23] A related objection to this proposal pertains to workability. First Amendment concerns aside, how would an ISP know if reported content actually constitutes a tort? What kind of proof should a purported victim present?

Implementing a notice and take-down scheme based on receiving actual knowledge (instead of constructive knowledge, or even strict liability) would help assuage these constitutional and workability-based concerns. In particular, imposing liability only for actual knowledge would limit collateral damage to protected forms of speech by not providing any incentive or requirement for ISPs to police the Internet. Instead, ISPs would retain immunity until they have actual knowledge through notice of the alleged tort. This limited scheme achieves the "[p]recision of regulation"[24] that the Supreme Court has required for rules implicating the First Amendment.

More generally, the danger of curbing speech protected by the First Amendment is not peculiar to ISPs and the Internet. If First Amendment concerns about regulating the Internet are justified, why are we not also worried that newspapers will decline to publish material for fear of legal liability? ISPs, like newspapers, obtain economic benefits by providing a forum for highly controversial material that will make it worth the risks to continue to do so in the future. Accordingly, First Amendment concerns may well be overstated.

Still, more tailoring is required to ensure workability—specifically, so that an ISP can fairly evaluate the notice it is given. A take-down scheme should

---

21. Professor Balkin has rightly predicted that safeguarding freedom of speech in the digital age will increasingly fall to governmental entities that can shape regulatory solutions that also secure the values of free expression. Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 6 (2004).

22. Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 30-31 (2006).

23. *Id.* at 65.

24. *See* NAACP v. Button, 371 U.S. 415, 438 (1963) ("Broad prophylactic rules in the area of free expression are suspect. . . . Precision of regulation must be the touchstone in an area so closely touching our most precious freedoms.").

only allow redress for torts that have relatively unambiguous elements. Though creating a bright line for determining exactly which torts would and would not fit this bill is beyond the scope of a short essay, there certainly would need to be some principled demarcation. Two torts that might be good candidates for regulation—based on their relatively unambiguous elements—are libel and public disclosure of private facts (a form of invasion of privacy). By way of example, a party requesting removal of libelous online content would need to provide sworn notification that she was being defamed and a detailed accounting of her claim that the assertion is both false and injurious to her reputation.[25] For the tort of public disclosure of private facts, a party seeking removal of harmful private facts would need to provide sworn notification explaining why the information is both highly offensive and not of legitimate concern to the public.[26]

After receiving notice of either of these torts, the ISP would need to disable or remove content (or have its customer remove content) or risk liability. As under the DMCA, where a notice does not sufficiently make the required showing, the ISP would not lose its immunity for the challenged content. This caveat should limit incentives to over-comply with take-down requests. Though any degree of Internet regulation is subject to possible abuses, limiting the regulation in this manner should ease the administrative burden for an ISP of determining whether to take down content based on notice—and curb the potential for companies to implement prophylactic measures simply to avoid liability.

Moreover, notice for these torts is not significantly more ambiguous than notice standards under the DMCA. For example, copyright infringement claims require an implicit affirmation that the material is not subject to a "fair use" defense, a doctrine that is not without ambiguities. Still, the DMCA has proved workable—even without absolute clarity.

A final objection might concern whether ISPs are best suited to gauge whether material is tortious and, hence, should be removed. This question of *how* ISPs respond to possible liability, however, is discrete and secondary to the

---

25. "[A] communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him." PROSSER AND KEETON ON THE LAW OF TORTS 774 (W. Page Keeton ed., 5th ed. 1984). This treatise later notes that "[d]efamation should be limited to imputations about the plaintiff that prove to be false and discreditable." *Id.* at 777.

26. *See* RESTATEMENT (SECOND) OF TORTS § 652D (1981) (setting out the elements of the tort of public disclosure of private facts); *see also* PROSSER AND KEETON ON THE LAW OF TORTS, *supra* note 25, at 857 ("The law is not for the protection of the hypersensitive, and all of us must, to some reasonable extent, lead lives exposed to the public gaze. . . . It is quite a different matter when the details of sexual relations are spread before the public eye, or there is highly personal portrayal of his intimate private characteristics or conduct.").

primary determination of *who* ought to shoulder financial responsibility. Vicarious liability in a free market leaves the choice of how to respond up to the target of liability.[27] Imposing vicarious liability on ISPs will create economic incentives for them to be sensitive to complaints about tortious material and ensure they have proper metrics in place for responding appropriately to take-down requests.

In sum, cyberlaw scholars have searched for how tort law can evolve to redress and deter cyberwrongs. And the DMCA is admittedly not a *perfect* model for imposing tort liability. However, imposing the limited liability sketched above would be a first step in requiring ISPs to take a more involved role in addressing torts in cyberspace.

Bradley A. Areheart is an attorney at Jenner & Block. The views expressed in this essay are his alone and do not represent those of the firm. *He thanks Seth Belzley, James Grimmelmann, Michael Heidler, Seth Kreimer, and Eric Posner for their very helpful comments.* *He may be contacted at bareheart@jenner.com.*

Preferred Citation: Bradley A. Areheart, *Regulating Cyberbullies Through Notice-Based Liability*, 117 YALE L.J. POCKET PART 41 (2007), http://thepocketpart.org/2007/09/08/areheart.html.

27. Reinier Kraakman, *Third Party Liability*, *in* 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 583, 585 (Peter Newman ed., 1998) (observing that vicarious liability "leaves the choice of whether and how to reduce [misconduct] entirely to the liability target").