1-2010

Section 230 of the CDA: Internet Exceptionalism as a Statutory Construct

H. Brian Holland
Texas A&M University School of Law, hbholland@law.tamu.edu

Section 230 of the CDA: Internet Exceptionalism as a Statutory Construct

By H. Brian Holland*

Introduction

Since its enactment in 1996, Section 230 of the Communications Decency Act has become perhaps the most significant statute in the regulation of online content, and one of the most intensely scrutinized. Many early commentators criticized both Congress, for its apparent inability to craft the more limited statute it intended, and the courts, for interpreting the statute broadly and failing to limit its reach. Later commentators focus more clearly on policy concerns, contending that the failure to impose liability on intermediaries fails to effectuate principles of efficiency and cost avoidance. More recently, commentators have argued that Section 230 immunity should be limited because it contributes to the proliferation of anonymous hate speech, intimidation, and threats of violence against traditionally marginalized groups.

Acknowledging the validity of these concerns, this essay nevertheless takes the opposing view, defending broad Section 230 immunity as essential to the evolving structure of Internet governance. Specifically, Section 230 provides a means of working within the sovereign legal system to effectuate many of the goals, ideals, and realities of the Internet exceptionalist and cyber-libertarian movements. By mitigating the imposition of certain external legal norms in the online environment, Section 230 helps to create the initial conditions necessary for the development of a modified form of exceptionalism. With the impact of external norms diminished, Web 2.0 communities, such as wikis[1] and social network services,[2] have emerged to facilitate a limited market in norms and values and to provide internal enforcement mechanisms that allow new communal norms to emerge. Section 230 plays a vital role in this process of

---

* Associate Professor, Texas Wesleyan School of Law. A modified version of this essay originally appeared in the University of Kansas Law Review. *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism,* 56 U. Kan. L. Rev. 369 (2008), **http://papers.ssrn.com/sol3/papers.cfm?abstract_id=979183**.

1 A wiki is a website designed to allow visitors to easily create and edit any page on the site. For more information, see Wikipedia, *Wiki*, **http://en.wikipedia.org/wiki/Wiki** (last accessed Dec. 1, 2010).

2 Social network services are online services designed for users to share messages, links, and media (photos and video) with friends or others with similar interests. Some popular social network services are Facebook, MySpace, and Twitter.

building heterogeneous communities that encourage collaborative production and communication. Efforts to substantially reform or restrict Section 230 immunity are therefore largely unnecessary and unwise.

The essay begins with a brief introduction to Section 230. As interpreted and applied by the judiciary, this statute is now conceived as a broad grant of immunity from tort liability—broad not only in terms of those who can claim its protection but also in terms of predicate acts and causes of action to which such immunity extends.

Working from this foundation, I then seek to position the courts' expansion of Section 230 immunity within the larger debate over Internet governance, suggesting that proponents of expanded immunity are successfully creating what might be characterized as a modified, less demanding form of cyber-libertarian exceptionalism than what Eric Goldman calls, in his essay in this book, the "First Wave of Internet Exceptionalism" (one of "Internet Utopianism"), as articulated in the mid-1990s. The dramatic expansion of Section 230 immunity has in a limited sense effectuated a vision of a community in which norms of relationship, thought and expression are yet to be formed. The tort liability from which Section 230 provides immunity is, together with contract, a primary means by which society defines civil wrongs actionable at law. In the near absence of these external norms of conduct regulating relationships among individuals, the online community is free to create its own norms, its own rules of conduct, or none at all. It is a glimpse of an emergent community existing within, rather than without, the sovereign legal system.

Finally, I make the case for preserving broad Section 230 immunity. As an initial matter, many of the reforms offered by commentators are both unnecessary and unwise because the costs of imposing indirect liability on intermediaries are unreasonable in relationship to the harm deterred or remedied by doing so. Moreover, the imposition of liability would undermine the development of Web 2.0 communities as a form of modified exceptionalism that encourages the development of communal norms, efficient centers of collaborative production, and open forums for communication.

The Expansion of Section 230 Immunity

In May of 1995, a New York trial court rocked the emerging online industry with its decision in *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[3] holding the Prodigy computer network liable for defamatory comments posted on one of its bulletin boards by a third-party. The key factor in this result was Prodigy's attempt to create a more family-friendly environment through the exercise of editorial control over the bulletin boards and moderating for offensive content.

---

[3] No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

Prodigy was therefore treated as a publisher of the information, rather than a mere distributor, and held strictly liable for actionable third-party content.

Representatives of the online industry argued that the Prodigy decision placed service providers in an untenable position by creating a "Hobson's choice"[4] between monitoring content and doing nothing, thereby insulating the service from liability. Congress responded to the decision by amending the draft Communications Decency Act (CDA) to include a tailored immunity provision addressing the online industry's concerns. As one element of what came to be known as the Good Samaritan provisions of the CDA, Section 230 was generally intended to provide online service providers and bulletin board hosts with immunity from tort liability for the defamatory acts of their users. This was accomplished by addressing those specific elements of common law defamation at issue in the Prodigy decision—editorial control and the distinct treatment of publishers and distributors under the law. To that end, Section 230 provided that no interactive computer service should be treated as the publisher or speaker of third-party content, and that efforts to moderate content should not create such liability.

In the years following the enactment of Section 230, courts consistently extended its application. This trend began in 1997 with the watershed decision in *Zeran v. America Online, Inc.*,[5] in which the Fourth Circuit applied Section 230 to claims that America Online (AOL) should be held liable for the defamatory content posted by one of its users. The plaintiffs claimed liability arose in part because AOL had allegedly failed to remove third-party defamatory messages from its bulletin board system within a reasonable time, refused to post retractions to defamatory messages, and failed to screen for similar defamatory messages thereafter. The court found the plaintiff's tort claims were preempted by Section 230, which rendered AOL immune. In reaching this result, the court rejected a strict reading of Section 230 as being limited to its terms. Although the statute failed to make any explicit reference to distributor liability, which the *Prodigy* decision appeared to leave intact, the court read distributor immunity into the statute, finding distributor liability to be an included subset of the publisher liability foreclosed by the statute. By collapsing the publisher-distributor distinction, the Fourth Circuit adopted the most expansive reading possible of both defamation law and Section 230. Thus, even though AOL knew the statements were false, defamatory, and causing great injury, AOL could simply refuse to take proper remedial and preventative action without fear of liability.

---

4 SAMUEL FISHER, THE RUSTICK'S ALARM TO THE RABBIES (1660), as cited in *Hobson's choice*, Wikipedia, **http://en.wikipedia.org/wiki/Hobson%27s_choice** (last accessed Dec. 1, 2010).

5 129 F.3d 327 (4th Cir. 1997).

Following *Zeran*, and building on that court's reading of both the statute and the policies sought to be effected, courts have extended the reach of Section 230 immunity along three lines: (1) by expanding the class who may claim its protections; (2) by limiting the class statutorily excluded from its protections; and (3) by expanding the causes of action from which immunity is provided.[6] As to the first, courts have interpreted the provision of immunity to interactive computer services to include such entities as Web hosting services, email service providers, commercial websites like eBay and Amazon, individual and company websites, Internet dating services, privately-created chat rooms, and Internet access points in copy centers and libraries. The additional provision of immunity to users of those services promises similar results. Already, one decision has held that a newsgroup user cannot be held liable for re-posting libelous comments by a third party,[7] while another court found a website message board to be both a provider and a user of an interactive computer service.[8]

The second line of extension results from a narrow reading of the term "information content provider," which defines the class for whom there is no immunity. Specifically, courts have held that minor alterations to third-party content does not constitute the provision of content itself, so long as the provider does not induce the unlawful content through the provision of offending raw materials of authorship and where the basic form and message of the original is retained.[9] The third point of expansion has been to extend Section 230 immunity beyond causes of action for defamation and related claims to provide immunity from such claims as negligent assistance in the sale/distribution of child pornography,[10] negligent distribution of pornography of and to adults,[11] negligent posting of incorrect stock information,[12] sale of fraudulently autographed sports memorabilia,[13] invasion of privacy,[14] and misappropriation of the right of publicity.[15]

---

6 *But see* Fair Housing. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (declining to extend Section 230 immunity to Roommates.com for certain categories of content solicited by the site for users in violation of federal fair housing laws).

7 Barrett v. Rosenthal, 146 P.3d 510, 527 (Cal. 2006).

8 DiMeo v. Max, 433 F. Supp. 2d 523, 531 (E.D. Pa. 2006).

9 Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003). *See also* Donato v. Moldow, 865 A.2d 711, 724 (N.J. Super. Ct. App. Div. 2005) (quoting *Batzel v. Smith*).

10 Doe v. Am. Online, Inc., 783 So. 2d 1010, 1017 (Fla. 2001).

11 Does v. Franco Prods., No. 99 C 7885, 2000 WL 816779, at *5 (N.D. Ill. June 22, 2000), *aff'd sub nom.* Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

12 Ben Ezra, Weinstein & Co. v. Am. Online, Inc., 206 F.3d 980, 986 (10th Cir. 2000).

13 Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 715 (Cal. Ct. App. 2002).

Section 230, Internet Governance & Exceptionalism

Situated within the larger debate over Internet governance, the concept of Internet exceptionalism presumes that cyberspace cannot be confined by physical borders or controlled by traditional sovereign governments, and thus that cyber-libertarian communities will emerge in which norms of relationship, thought and expression are yet to be formed. Although these ideas have been subjected to intense criticism and somewhat obscured by recent developments in the governance debates, they remain a touchstone for the cyber-libertarian ideal. This part of the essay seeks to clear space in the governance debates for this vision of exceptionalism, and argues that Section 230 is in some limited way facilitating the emergence of cyber-libertarian communities in a modified, less demanding form.

Foundational Arguments of Internet Governance

The debate over Internet governance evolved in two surprisingly distinct, albeit convergent stages. The first stage of the governance debate focused on law and social norms, and whether these traditional models of regulating human relations could be validly applied to the online environment. In this context, exceptionalism was conceptualized as a state of being to which the Internet had naturally evolved, apart from terrestrial space. The second stage of the debate introduced network architecture as an important and potentially dominant means of regulating the online environment. In this context, exceptionalism became an objective to be pursued and protected as a matter of choice, rather than a natural state. At a more exacting level, these debates implicated fundamental questions of legitimacy, preference, politics, democracy, collective decision-making, and libertarian ideals.

In the early 1990s, as the Internet began to reach the masses with the advent of the World Wide Web, a particular vision of the online environment emerged to advocate and defend Internet exceptionalism. Described as digital libertarianism or cyber-libertarianism, the vision was one of freedom, liberty, and self-regulation. Cyber-libertarians believed the Internet could and would develop its own effective legal institutions through which rules would emerge. These norms would emerge from collective discourse around behavior,

---

14 Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124 (9th Cir. 2003).

15 *See id.* at 1122, 1125 (extending § 230 immunity to defendant in claim "alleging invasion of privacy, misapproriation of the right of publicity, defamation and negligence"). *See also* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1118–19 (9th Cir. 2007) (finding that § 230 immunity extends to state-law intellectual property claims, including unfair competition, false advertising, and right of publicity).

relationship, and content, rather than from the control and regulation of network architecture. Control of architecture was seen almost exclusively as an instrument by which to enforce emerging social norms, and not as a means of determining the norms themselves. By the mid-1990s this process of self-regulation was well underway.

At the same time, however, sovereign nations and their constituents increasingly sought to impose existing offline legal regimes on this emerging, resource-rich environment. Many in the online community resisted, perceiving this regulation as a threat to the exceptional nature of the Internet. Advocates of self-regulation envisioned cyberspace as a distinct sphere, apart from physical space. These cyber-libertarian exceptionalists saw the imposition of existing offline legal systems grounded in territorially-based sovereignty as inappropriate. They believed that the online environment should instead be permitted to develop its own discrete system of legal rules and regulatory processes. Self-regulation was preferable in its own right because it had proven so effective in creating the environment sought to be preserved, and also because the alternative seemed devastating. The imposition of external, territorially-based legal regimes would be, the exceptionalists argued, infeasible, ineffective, and fundamentally damaging to the online environment.

Faced with the attempted imposition of offline legal regimes, cyber-libertarians responded by attacking the validity of exercising sovereign authority and external control over cyberspace. According to Professors David Johnson and David Post, two leading proponents of self-governance, external regulation of the online environment would be invalid because Internet exceptionalism—the state of being to which the Internet naturally evolved—destroys the link between territorially-based sovereigns and their validating principles of power, legitimacy, effect, and notice.[16] Most importantly, the Internet's decentralized architecture deprives territorially-based sovereigns of the power, or ability, to regulate online activity. Likewise, extraterritorial application of sovereign law fails to represent the consent of the governed, or to effectuate exclusivity of authority based on a relative comparison of local effects. The loss of these limiting principles results in overlapping and inconsistent regulation of the same activity with significant spillover effect. Deprived of these validating principles, it would be illegitimate to apply sovereign authority and external control in cyberspace.

---

[16] David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367 (1996).

A primary challenge to these cyber-libertarian arguments came from Professor Goldsmith, who engaged both their descriptive and normative aspects.[17] In terms of the legitimacy of sovereign regulation, Goldsmith criticized Johnson and Post's limited view of sovereignty and over-reliance on the relationship between physical proximity and territorial effects. Moreover, he argued that they had overstated the impossibility of regulation, mistaking ability for cost; failed to recognize the deterrent effect on extraterritorial actors of local enforcement against end users and network components located within the territory; and mistakenly equated valid regulation with some measure of near-perfect enforcement. Finally, where true conflicts between sovereigns existed, Goldsmith argued that these could be resolved with the same tools used in the offline world—rules of jurisdiction, conflict of laws, enforcement, *etc.* Throughout, Goldsmith struck at Johnson and Post's exceptionalist view of the Internet, implicitly rejecting the ultimate significance of both the technical and communal aspects of that ideal. This critique proved devastating to these early cyber-libertarian arguments.

The governance debate entered its second phase in 1999 with the publication of Professor Lessig's book, *Code and Other Laws of Cyberspace*.[18] Prior to Lessig's book, the governance debate had focused primarily on behavioral and property norms, with the assumption that either existing sovereign law or the law emerging from Internet self-governance would prevail. Network architecture merely provided the means to enforce these norms, particularly those emerging from self-governance. Lessig reconceived Internet exceptionalism as a two-part phenomenon, one regulatory and the other cultural. The former recognizes that many of those features that make the Internet exceptional (in the cyber-libertarian sense) are merely coding choices, and not the innate nature of cyberspace. Within the network, architecture and code are the most basic forms of regulation. Code can be easily changed. Thus, Lessig argued, to protect the cultural aspects of exceptionalism, we must first recognize the exceptional regulatory power of architecture and code within cyberspace, and its pivotal role in preserving or destroying that culture.

Lessig first pointed out that law and social norms are but two means of regulating human behavior. In cyberspace, unlike real space, it is possible for architecture to dominate regulatory structures. Architecture acts as a regulator in the offline world as well—in the form of time, nature, physics, *etc.*—but our laws and social norms are generally conceived with these regulators assumed. Alteration of that architecture is unusually difficult if not practically impossible. In cyberspace, by comparison, architecture in the form of code is remarkably

---

17 Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. Chi. L. Rev. 1199 (1998); Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 Ind. J. Global Legal Stud. 475 (1998).

18 LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

fluid. Code effectuates a series of choices, from data collection, to anonymity, to access. And code can be changed. Not only is code fluid, but within cyberspace it is a uniquely powerful form of regulation. Rather than regulating behavior and relationships through punishment, deterrence and post-violation corrective action, code provides the means to exercise perfect control and thus perfect regulation—regulation not just of effects, but of the very universe of choices from which an individual actor is able to select.

With this shift in focus, the debate itself evolved. Lessig cautioned that the greatest threat to the exceptional culture of cyberspace comes from the union of perfect control and market forces of commerce. The architectural components that provide the means of perfect control are held almost exclusively by private entities with commercial and political interests distinct from the collective. The invisible hand, Lessig argued, cannot resist the promise of perfect control, and has little or no motivation to protect the fundamental values promoted by cyber-libertarian exceptionalism. According to the cyber-libertarian narrative, barriers that are present in the real world do not exist or are *de minimus* in the online environment. In the context of Internet architecture, exceptionalism can be found in original principles of network design that rely on open protocols and non-discriminatory data transfer—a network that is decentralized, borderless, and with the potential for nearly unlimited data capacity. Indeed, the digital data flowing through this system is itself exceptional, because it is easy to create and manipulate, easy to copy with no degradation in quality, and easy to access and distribute. In the context of online relationships, exceptionalism resides (at the very least) in the interactivity, immediacy, and potential scope of interaction, as well as the opportunity for anonymity. However, the very promise of perfect control is to eliminate many of these choices and the fundamental values they reflect as subservient to commercial goals. In cyberspace, control over coded architecture supplies the means for making this election. Building on this assertion, Lessig argued that in order to protect fundamental values, decisions regarding architecture should emerge from the body politic and collective decision-making, rather than being concentrated in private actors.

For many cyber-libertarians, Lessig's message presented great problems. Although many had already abandoned the argument that the exercise of sovereign authority in cyberspace was normatively invalid, they had not given up (as a matter of preference) the vision of an emergent, self-governed, digital libertarian space. Sovereign legal regimes were still seen as the greatest threat to that vision. Territorial governments should, the cyber-libertarians argued, simply leave cyberspace alone to flourish. From this perspective, Lessig's arguments about the unique regulatory power of architecture and code in cyberspace were largely convincing. But his description of the corrupting influence of perfect control and concentrated private power, and particularly his

call for government regulation to counteract those influences and preserve fundamental values, were difficult to square with most libertarian views.

The debate on net neutrality provides a glimpse of this division. Many commentators, including Lessig, are concerned that the private owners that control the physical/infrastructure layer of the network will, in pursuit of cross-layer vertical integration and increased revenues, privilege certain content or applications. They therefore endorse regulatorily-mandated neutrality as a means of preserving one aspect of Internet exceptionalism. Not surprisingly, many libertarians reject this approach, endorsing instead market-based solutions for effectuating individual choice.

The irony of this debate is fairly apparent. Many who might otherwise have characterized themselves as cyber-libertarian, or at least sympathetic to that vision, are now conflicted. Net neutrality would necessarily be imposed by external sovereign legal systems and subordinated to the control of commercial entities, rather than emerging as a common norm. In the extremes, the issue seems to present a choice between entrenched political power and unregulated market forces, with neither providing adequate protection for individuals. Thus, many of the Internet exceptionalists who sought to segregate the Internet from territorial boundaries, who assumed existing sovereign governments and legal regimes were the greatest threat to the online community, who believed that the computer scientist would remain in control of the network (and thus in control of enforcement), found themselves asking Congress to protect the Internet from private actors and market forces.

What's Left of Exceptionalism?

What then is left of Internet exceptionalism? In his revolutionary essay *A Declaration of the Independence of Cyberspace*, John Perry Barlow described cyberspace as consisting not of computers, wires, or code, but of "transactions, relationships, and thought itself."[19] It was this vision, this perception of an evolving social space, that guided Barlow's ideal of the culture he sought to preserve—a distinct vision of potential worthy of protection. Indeed, to many early inhabitants of cyberspace, communal control and regulation of network architecture appeared a given, if for no other reason than that perfect external control seemed almost impossible. Freedom of choice in individual expression, human behavior, and relationships were the heart of the online cultural and social ideal that stirred Barlow and other cyber-libertarians.

As it evolved, the governance debate fractured this largely unified vision, distinguishing validity from preference, law and social norms from architecture

---

[19] John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb. 8, 1996), **http://homes.eff.org/~barlow/Declaration-Final.html**.

and code, technical exceptionalism from cultural exceptionalism, government power from private commercial power, and even libertarian from libertarian. Lessig argued persuasively that the greatest threat to digital libertarianism arose from private actors, unbounded by fundamental values (including constitutional values) and with the ability to exercise perfect control over choice. Lessig's analysis, generally speaking, was focused on the treatment of data as data, based primarily on the identity of its owner and the commercial interests represented. Choice in action was to be controlled by the regulation of owned data, discriminatory treatment of data to the benefit of certain owners, restriction of network access, and similar means. These technical controls would then be bolstered by traditional sovereign law validating those measures.

What seems somewhat obscured in Lessig's architecture-and-code approach (which clearly remains the central concern of the governance debate) is Barlow's original vision of relational libertarianism, with its focus on expression of individual choice and the development of new communal social norms within a system of self-governance. This is the part of Internet exceptionalism that was, in a sense, overwhelmed by the debate over architecture and code. Yet there are some choices, primarily relational, that remain largely unaffected by that debate. In this sphere, the question is not access to choice, the ability to choose, or the available universe of choices, but rather what norms apply to the choices being made outside those controls.

Post argues that fundamental normative values could "best be protected by allowing the widest possible scope for uncoordinated and uncoerced individual choice among different values and among different embodiments of those values."[20] He believes that the imposition of sovereign legal regimes in cyberspace, rather than promoting fundamental values as Lessig argued, would instead deny the digital libertarian culture the opportunity to develop apart from the offline world, with its own set of fundamental values. He argues it is better to serve the private interest (even if powerful and commercially motivated) than the interest of terrestrial sovereigns. Indeed, he sees exceptionalism as requiring self-governance, to the exclusion of external legal norms imposed by sovereign powers, as a precondition to the emergence of a new system of norms.

Section 230 as a Form of Cyber-Libertarian Exceptionalism

Most would say that Barlow and Post lost the battle. However, this particular strain of Internet exceptionalism, envisioned as self-governance and emerging social norms applicable to relationships between individuals (as opposed to data as data), has been preserved in a modified, less demanding form. Ironically, it is because of sovereign law, not in spite of it, that this occurred. The dramatic

---

20 David Post, *Against "Against Cyberanarchy*," 17 Berkeley Tech. L.J. 1365 (2002).

expansion of Section 230 immunity has effectuated many of the ideals promoted by Post, Barlow, and others, albeit on a limited scale. This expansion has created an environment in which many of the norms and regulatory mechanisms present in the offline world are effectively inapplicable. This is so not because the very nature of cyberspace makes such application impossible, or because sovereign law is necessarily ineffective or invalid, but rather because sovereign law has affirmatively created that condition.

The torts for which Section 230 provides immunity are, together with contract law, the primary means by which society defines civil wrongs actionable at law. These norms of conduct regulate relationships among individuals: articulating wrongs against the physical and psychic well-being of the person (*e.g.*, assault, battery, emotional distress), wrongs against property (e.g., trespass to land, trespass to chattels, conversion), wrongs against economic interests (e.g., fraud, tortious interference), and wrongs against reputation and privacy (e.g., defamation, misappropriation of publicity, invasion of privacy). Section 230 has been interpreted and applied to provide expansive immunity from tort liability for actions taken on or in conjunction with computer networks, including the Internet. Statutory language defining who may claim the protections of Section 230 immunity, including providers of interactive computer services and the users of such services, has been broadly extended. In contrast, the primary limitation on the range of claimants to Section 230 immunity, which is statutorily unavailable to the allegedly tortious information content provider, has been construed fairly narrowly. Moreover, the immunity provided to this expansive cross-section of online participants now reaches well beyond defamation to include a wide range of other tortious conduct and claims. As such, many of the norms of conduct regulating relationships among individuals in the offline world—those civil wrongs actionable at (tort) law—simply do not apply to many in the online world.

Even where the online entity is alleged to be aware of the illegal acts of their users, and to be either actively facilitating those illegal acts or refusing to stop them, the intermediary retains Section 230 immunity. This is true even where the intermediary has the knowledge, technical ability, and contractual right to take remedial action. In the offline world, such active and knowing facilitation would likely violate social norms established in tort law. In the online world, however, the defendants are immune from liability. Established norms, as expressed through the mechanisms of tort law, are neutralized by Section 230 and its judicial interpretations.

In the near absence of these external legal norms, at least within the range of choices being made outside the data-as-data architectural controls, the online community is free to create its own norms, its own rules of conduct, or none at all. The inhabitants may not have a blank slate—criminal law, intellectual property law, and contract law still apply—but much of what Barlow embraced

as central tenets (mind, identity, expression) remain undefined. Section 230 offers a modified version of cyber-libertarian exceptionalism, less demanding of the sovereign and existing offline social norms, and therefore less satisfying. But it is nonetheless a glimpse of that society, maintained by the sovereign legal regime rather than against it. The law now applies to nearly every tort that can be committed in cyberspace. It is nibbling at the edges of intellectual property rights. It protects against the civil liability components of criminal acts. It generally extends to all but the first speaker, who may well get lost in the network to escape liability even without immunity.

A Case for Preserving Section 230 Immunity

As interpreted by the courts, the immunity provisions of Section 230 have been heavily criticized. Many commentators have argued that by failing to impose indirect liability on intermediaries, significant harms will go undeterred or unremedied, and that Section 230 should be reformed to serve the interests of efficiency and cost allocation. This part of the essay addresses these criticisms directly, concluding that substantially reforming the statute is both unnecessary and unwise because the cost of such liability is unreasonable in relation to the harm deterred or remedied. Indeed, given Section 230's role in facilitating the development of Web 2.0 communities, reforming the statute to narrow the grant of immunity would significantly damage the online environment—both as it exists today and as it could become.

Evaluating Calls for Reform

Early critics of Section 230 tended to focus on the issues of congressional intent and broad interpretation by the courts. More recent commentators have moved beyond these issues to engage the larger implications of providing such sweeping immunity to online intermediaries, suggesting amendments to Section 230 intended to effectuate policies of efficiency and cost allocation. This critique begins with the premise that in the online environment, individual bad actors are often beyond the reach of domestic legal authorities. This creates a situation in which significant individual harms cannot be legally deterred or remedied, and the fear that the Internet's potential as a marketplace will not be realized. Given these negative conditions, where a third party maintains a certain level of control, the imposition of indirect liability is desirable. The failure to do so may create inefficiencies by failing to detect and deter harmful behavior where the cost of doing so is reasonable. Commentators have argued that, in the online environment, intermediaries are in the best position to deter negative behavior, to track down primary wrongdoers, and to mitigate damages. This is particularly true in regard to information-based torts, the damages of which might be mitigated in many circumstances simply by taking down, prohibiting, or blocking the objectionable content.

At the heart of this attack on Section 230 immunity is the idea that, in the absence of indirect intermediary liability, significant harms will go undeterred or unremedied. These fears are either misplaced or overstated. As an initial matter, it is not clear that a significant number of bad actors are beyond the reach of the law. Advances in technology are making it increasingly possible to locate and identify bad actors online, such that online anonymity is difficult to maintain. Likewise, where the bad actor is identified but is found outside the jurisdiction, sovereign governments have developed methods for resolving disputes to permit the direct extraterritorial application of domestic law, such as rules of jurisdiction, conflict of laws, and recognition of judgments. Indeed, anti-exceptionalists have strenuously argued that the application of sovereign authority to online activity originating outside the jurisdiction is legitimate and valid in large part because of these rules.

Moreover, although the immunity provided by Section 230 arguably mitigates the legal incentives for online intermediaries to deter and remedy certain negative behavior, it does not eliminate those legal incentives. Section 230 expressly states that it has no effect on criminal law, intellectual property law, or communications privacy law. These external norms remain applicable to and enforceable against both content providers and intermediaries in the online environment. Perhaps even more significantly, although Section 230 removes legal incentives to enforce the norms expressed in tort law, law is certainly not the only incentive for an intermediary to act. Communal, commercial and other incentives also play a role. Indeed, Section 230 immunity allows intermediaries the freedom to intervene in a multitude of ways. Thus, individual harms and marketplace security can be addressed through alternate legal regimes and internal incentives.

Furthermore, proponents of indirect intermediary liability concede that even where harms do exist, intermediaries may only rightly be held liable for failing to detect and deter harmful behavior where the cost of doing so is reasonable. It is unclear, however, that the costs of intermedial regulation are reasonable. In terms of remedies and reforms, critics generally suggest some form of the detect-deter-mitigate model, imposing a duty upon the intermediary with the potential for liability in cases of breach. The two most common models are traditional liability (damages) regimes and notice-and-takedown schemes. Proponents of traditional liability schemes generally find theoretical fault with the exceptionalist view of the Internet, and analytical fault with broad judicial interpretations of the statute that collapse distributor-with-knowledge liability into immunity from publisher liability. Proponents of a notice-and-takedown scheme likewise work from a distributor-with-knowledge model that imposes a limited duty of care on intermediaries, but generally acknowledge some degree of exceptionalism that requires a distinct scheme. Most suggest some variation

utilizing elements of the Digital Millennium Copyright Act (DMCA)[21] and the European Union's E-Commerce Directive,[22] wherein intermediary liability is triggered by actual notice of the objectionable content or a standard of reasonable care, and requiring remedial action (e.g., taking down the content at issue).

The costs of these indirect intermediary liability schemes could be great. Under traditional liability rules, intermediaries may be forced to adopt a least-common-denominator approach, resulting in overly-broad restrictions on expression and behavior. A modified distributor-with-knowledge approach, usually in the form of a takedown scheme similar to that employed by the DMCA, may produce the same type of chilling effect. This is potentially exacerbated by the use of a should-have-known standard that can trigger the need to patrol for harmful content, raising costs and leading to even greater overbreadth in application. Moreover, indirect liability reduces incentives to develop self-help technology, such as location or identity tracking software and end-user filters, the development of which was one of Section 230's primary policy goals. Thus, if the scale of undeterred or unremedied harms is minimal, and the negative impact of a detect-deter-mitigate model is significant, then the cost associated with the imposition of indirect intermediary liability is not reasonable.

Resisting the Urge Toward Homogeny

The case for preserving Section 230 immunity begins by recasting intermediary immunity in terms of exceptionalism, self-governance and norms, because it is precisely the gap between the offline social norms expressed in tort law and the broad immunity provided to online participants that has led to the rather strong criticism of Section 230. As a conceptual matter, communal enforcement presents the greatest challenge to effectuating some modified version of the exceptionalist ideal. When external legal norms are excluded, internal enforcement mechanisms facilitate the emergence of new communal norms to take their place. Much of the criticism of Section 230 stems from the lack of legal enforcement that accompanies immunity, and the resulting inability to form new social norms to replace those of the sovereign. It is important to recognize, however, that Web 2.0 communities, such as wikis and social networks, represent a real and significant manifestation of the exceptionalist vision, because they both facilitate a market in norms and values, and provide the internal enforcement mechanisms necessary for internal norms to emerge. Section 230 plays a vital role in the development of these communities by

---

21 Digital Millenium Copyright Act, Pub. L. 105-304, 112 Stat. 2860 (1998).

22 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT**.

substantially and continually mitigating the primacy of external legal norms within the confines of the community. This permits choice, empowers the intermediary to create a market in social norms, and allows alternate forms and gradations of enforcement. The architecture of the community gives these choices form and substance, backed by an enforcement model, such that communal norms have the opportunity to develop. In this sense, Section 230 and the Web 2.0 model effectuate the emergence of a modified form of exceptionalism. The reforms proposed by most commentators would have a negative impact on these communities, with little benefit beyond those communal norms that are likely to emerge, and should be rejected.

Exceptionalism, Self-Governance & Social Norms

Exceptionalism does not argue for the absence of social norms. Instead, exceptionalism embraces the idea of cyberspace as an environment in which the authority of external legal regimes is minimal, and where an open market in norms and values works in concert with self-governance to permit the online community to establish its own substantive social norms. Section 230 helps to effectuate a modified form of exceptionalism by moderating the imposition of external legal norms so as to permit a limited range of choices—bounded, at least, by criminal law, intellectual property law and contract law—in which the online community is free to create its own norms and rules of conduct. However, the development of social norms within this environment requires not only the ability to exercise broad individual choice among different values and embodiments of those values, but also some mechanism of communal enforcement through which to effectuate some form of self-governance.

Early proponents of exceptionalism were able to focus on relational libertarian ideals, viewing the Internet as a unique social space in which norms governing thought, expression, identity, and relationship should be permitted to evolve. This focus developed precisely because the mechanisms of enforcement required for self-governance and the evolving definition of emergent social norms were taken for granted. The architecture of enforcement was primarily controlled by a community involved in the process as adherents to the exceptionalist ideal, who could be trusted both to ensure broad individual choice and to utilize the means of enforcement as a tool of self-governance as norms emerged.

As a means of effectuating exceptionalism, the primary weakness of Section 230 is the lack of an enforcement component. Although the modified exceptionalism enabled by Section 230 permits a range of choices, it does nothing to provide enforcement mechanisms to solidify emerging communal norms. Where immunity exists, legal enforcement mechanisms are never triggered. Likewise, the architecture of enforcement relied upon by early exceptionalists is no longer communal or likely committed to the vision of a distinct cyber-libertarian space, but is instead concentrated in private

commercial entities. As a consequence, Section 230 immunity creates a gap: Certain external legal norms are excluded, but internal communal norms are often unable to coalesce to take their place. It is this gap, resulting from the lack of architectural enforcement controls, which fuels criticism of the immunity provision. In application, however, an enforcement model has emerged that mediates the tension between the broad availability of individual value choices and the ability to effectively self-govern so as to permit the development of communal norms.

Communities of Modified Exceptionalism

Web 2.0 communities are structured as a limited commons and are built on an architecture of participation that operates as a platform for user-created content and collaboration. At the core are principles of open communication, decentralized authority, the freedom to share and re-use, and an idea of the Internet as a social forum or market for exchanging opinions and ideas in search of norms to create a culture based on sharing. Section 230 plays a vital role in the development and maintenance of these architectures by providing intermediaries with limited immunity from liability for the tortious content provided by users. Indeed, in this sense, Section 230 seems to favor the development of Web 2.0 services and the provision of user-based content over the traditional model of providing first-party institutional content.

The parallels between Web 2.0 and Barlow's vision of a communal social space are evident, albeit in modified form. Barlow embraced the potential of an environment premised upon freedom of choice in individual expression, human behavior and relationships. To achieve that potential, he and others believed that regulation by existing sovereign powers must be rejected in favor of self-governance, so that new communal social norms might have the opportunity to emerge. At the heart of this ideal was an affirmation that values participation in the market of expression, ideas and action without the constraint of preconceived value judgments. Web 2.0 promises a somewhat limited version of this environment—existing within sovereign authority, narrowed by certain enduring norms, and confined to segmented communities administered by private entities—by facilitating the market by which norms are tested.

Two of the most common models of these Web 2.0 services, wikis and social networks, are indicative of how Section 230 can effectuate the modified form of cyber-libertarian exceptionalism described above. Partly as a result of the immunity from liability provided by Section 230, these services facilitate the market in social norms by creating enclaves in which users may exercise broad (although not unbounded) individual choice among competing values. At the same time, the intermediary retains control over the architecture and thus the means of enforcement. As the market defines social good through the evolution of communal norms, that architecture may be employed as a mechanism of governance. In the absence of legal incentives, the enforcement

of communal norms is driven by internal incentives, such as the need for financial support from community donations, a communal desire for information integrity, or the need to build an audience for advertising. In some communities, participants may be incentivized by credibility and stature in the form of temporal seniority, post count, rank within the community's governing body, etc.

The online encyclopedia Wikipedia is a specific example of a Web 2.0 community of collective action. Each entry in the Wikipedia database is created and edited by volunteers who are guided by three primary principles: the Neutral Point of View policy, the No Original Research policy, and the Verifiability policy. Registered users can originate new articles, and any user, whether registered or anonymous, can edit an existing article. In the period between Wikipedia's inception in 2001 and 2010, this experiment in voluntary collaborative action produced more than ten million articles.

These activities are overseen by two levels of administrators, administrators and bureaucrats. Administrators (historically called sysops, short for system operators) have the power to edit pages, delete or undelete articles and article histories, protect pages, and block or unblock user accounts or IP addresses. Bureaucrats have the further power to create additional sysops with the approval of the community. In February 2006, in response to a series of significant and persistent acts of vandalism, the co-founder of Wikipedia created an additional layer of protection: Administrators can protect any article so that all future changes must be approved by an administrator.[23] Administrators help facilitate dispute resolution and enforcement. Low-level disputes are resolved in talk pages. Here, moderators guide members to resolution with reference to policies and guidelines developed over the life of the community. Thus, principle values and norms can lead to more specific rules. This approach works in most cases. More serious violations, such as malicious editing of an article (or vandalism), are addressed through fast-repair mechanisms executed by community members. Wikipedia administrators are also able to block user accounts or IP addresses.

As described, the Wikipedia community reflects a modified form of the exceptionalist model, initially allowing for individual choice among a range of values, facilitating a market in social norms, and providing a means of enforcement to effectuate norms as they develop. Indeed, recent studies reflect not only that norms have emerged from this market, but that those norms have solidified and expanded. Through this process, the Wikipedia community is

---

23 *See* Wikipedia, *Wikipedia: Protection Policy*, **http://en.wikipedia.org/wiki/Wikipedia:Protection_policy** (last accessed Dec. 1, 2010).

moving from an immediate focus on particular articles to more generalized concerns for quality of content and community.

Not unexpectedly, open source projects such as Wikipedia are not immune to abuse. In terms of community health, and to protect against these abuses, Wikipedia has adopted a code of conduct and principles of etiquette that stress civility and discourage personal attacks. As discussed above, these norms are enforced through an architecture that is designed to reinforce those norms with an eye towards the health of the community. At the most basic level, this occurs through routine editing by participants. Over time, more complex mechanisms for dispute resolution and enforcement have developed, such that in the past few years administrative and coordination activities have gained importance.

The relationship between architecture and social norms is fascinatingly apparent both in the Wikipedia's architectural choice to track and correlate the IP address of any anonymous user who edits the encyclopedia, as well as the development of a monitoring system that tracks those changes for analysis. This system serves as a mechanism for enforcing social norms, particularly the norm of neutrality in more controversial areas. In terms of more formal enforcement, some edits that might previously have been overlooked are now being reexamined in light of the organization from which they originated. Less formally, but perhaps even more effectively, organizations which are perceived to have breached the norms of the community have faced, and will face, recriminations. Moreover, the entire community is now aware that enforcement of those norms is now more effective, presumably creating a deterrence effect.

The Wikipedia example illuminates a constant process, as choices are narrowed by communal norms that develop and are given life through enforcement mechanisms, such that principle norms generate a breadth of more particular rules. Section 230 immunity plays an important role in this process, permitting the community to evolve and structure itself in the most efficient manner. To a limited extent, Section 230 immunity permits uncoordinated and uncoerced individual choice among different values and among different embodiments of those values. It further allows the intermediary to play an active role in facilitating the market in social norms and in creating enforcement mechanisms as a tool of self-governance. Those enforcement mechanisms can then themselves adapt. This allows not only for the development of distinct community values, but also for a means of tapping into incentives, adapting to evolving norms and conditions, and reducing costs associated with disputes. Within this framework, greater variations in community norms are possible. As communities grow, niche communities are formed at low cost. It is not the global vision of early exceptionalism, but rather a more limited and localized form of modified exceptionalism that functions as a laboratory for testing social norms and values.

Conclusion

Critics of Section 230 have both overstated the harms arising from immunity and understated the costs of alternate schemes for imposing indirect liability on online intermediaries. At the same time, they have ignored the important role Section 230 plays in the development of online communities. The immunity provided by Section 230 helps to create the initial conditions necessary for the development of a modified form of exceptionalism by mitigating the effect of external legal norms in the online environment. Web 2.0 communities are then able to facilitate a market in norms and provide the architectural enforcement mechanisms that give emerging norms substance. Given Section 230's crucial role in this process, and the growing importance of Web 2.0 communities in which collaborative production is yielding remarkable results, reforming the statute to substantially narrow the grant of immunity is both unnecessary and unwise.