Before the
UNITED STATES DEPARTMENT OF COMMERCE
Washington, D.C. 20230

GLOBAL FREE FLOW OF INFORMATION ON THE INTERNET

Comments of Nicholas Bramble
Information Society Project at Yale Law School*

Nicholas W. Bramble
Information Society Project at Yale Law School
127 Wall Street
New Haven, CT 06511
nicholas.bramble@yale.edu

December 6, 2010

* Nicholas Bramble is a Lecturer in Law at Yale Law School and a MacArthur Media Fellow at the Yale Information Society Project.

INTRODUCTION

The following comments are responsive to the Department of Commerce's Notice of Inquiry into the *Global Free Flow of Information on the Internet*, and specifically to the section entitled "The Role of Internet Intermediaries."

As the Department of Commerce has recognized, the services provided by Internet intermediaries "are integral to the growth and vitality of the Internet because they allow widespread user participation with minimal upfront costs or technical resources." Compared to actors on vertically integrated, linked-layer networks, innovators on the Internet act in a far more distributed and, in an important sense, *free* fashion without needing to be linked in to existing players and powerful network or content providers. The degree of user freedom on the Internet has important consequences as to expanding the scope of those who are able to access and participate in democratic governance, in electronic commerce, and in various additional forms of networked social, political, and religious organizations.

As the Department of Commerce seeks to reduce restrictions on the free flow of information on the Internet, then, it should concentrate on promoting and disseminating the legal conditions and structures that have allowed innovative intermediaries and users to flourish on the Internet.

But the legal structure underlying the development of the Internet is not necessarily intuitive, and should not be assumed to be on point with other mechanisms for promoting the progress of science and useful arts. In some sense, the laws and regulations responsible for the evolution of information flow on the Internet bear little resemblance to the models of creativity and innovation familiar from copyright and patent laws. Instead, the user-generated Internet as we know it today can be described as the result of (a) legislative safe harbors protecting network providers from liability for the content and applications they transport and (b) regulatory standards built upon a layered Internet architecture to promote interconnection of disparate networks and prevent network providers from using property rights or private regulatory mechanisms to stifle competition at the higher layers of content and applications. Together, in a rough sort of conjunction, these safe harbors and regulatory standards have transformed the Internet from a merely digital space into a fully networked space. Such mechanisms represent a shift from a model of information production based solely on exclusive rights towards a model more concerned with the cultivation and agricultural stewardship of information and applications from distributed sources.

I. Safe Harbors

Congress played a strong and influential role in the earlier days of the Internet by setting up safe harbors along the lines of Section 512(c) of the Digital Millennium Copyright Act and Section 230(c) of the Communications Decency Act – which permit platform providers to solicit, aggregate, and distribute content generated by users without thereby becoming legally responsible for that content. These safe harbors are based in

abstention and intentional under-enforcement of laws regulating creative production, privacy, and integrity of identity. Two concerns underpin DMCA § 512(c) and CDA § 230(c): the technical difficulty that website and network providers would face in monitoring user-generated content, and the intuition that a high amount of networked speech and user-generated content on the Internet represents a positive social outcome.[1]

Both DMCA § 512(c) and CDA § 230(c) risk a lot of creation on the boundaries of copyright law and defamation law, on the theory that the rewards of such creation – new structures and functions for online communities, as with Wikipedia,[2] YouTube, and Facebook; greater flourishing of interactive media; more robust political discourse; distribution and transformation of cultural works by diverse and antagonistic audiences – outweigh the risks of inefficient policing of violations of copyright, defamation, and obscenity law. These safe harbors reflect an implicit calculus that even if the hosts and providers of platforms and websites are *capable* of monitoring their sites for infringing or defamatory content (more capable, for instance, than an external party lacking equivalent access to sitelogs and other website analytics), the costs of imposing such a monitoring obligation on a service provider would stifle the benefits associated with the continued decentralized development of such services.

At the same time, it is clear that the technological architecture common to many sites on the Internet – an architecture premised on unmoderated user contributions, continuous edits, and shifting, unpredictable links – would not be readily adaptable to a world of intermediary liability:

> If we forced Google to try to find out which Web pages have problematic materials on them, there is no way it could return automated search results. Even if it employed an army of lawyers to scrutinize all of the content, it would still be in no position to tell which pages were infringing or defamatory. And even if it somehow figured out the answer for any given search result, it would have to determine the answer anew each time the search was run, because Web pages change frequently.[3]

And Google is not the only content, search, or application provider that would run into significant trouble in analyzing all of the user-generated information it finds. A site like Facebook or Twitter, premised on more immediate social interactions, often lacks an easy entryway for even the site's own administrators to peer deeply into social conversations taking place on the site. Legislation that would repeal existing safe harbors from intermediary liability would make things very difficult for these sorts of sites premised on quick, real-time conversations: it would effectively place the administrators of such sites in the position of live television censors seeking to ensure that all obscene or offensive

---

[1] *See* CDA § 230(a)(3) (finding that "[t]he 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").

[2] *See* Ken S. Myers, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. J. LAW & TECH. 163 (arguing that a proper interpretation of the CDA § 230 safe harbor immunizes Wikipedia from defamation liability).

[3] Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 102 (2007).

content was bleeped out during the short time period between its utterance and its broadcast. The destruction of safe harbors might also force such administrators to spend additional time uncovering and peering into otherwise hidden conversations on their sites, and might consequently run afoul of users' privacy expectations and settings.

Thus the common rationale for "abstention" from enforcement of copyright and defamation laws is partially a function of the practical difficulty of enforcing consistent obligations in a shifting technological context, and partially a function of a decision to promote greater user participation in culture and political discourse. The Department of Commerce should keep this dual rationale in mind when determining how best to promote new intermediary services and encourage responsible conduct by intermediaries.

II. Preserving Safe Harbor Diversity

Citing the effectiveness of the common rationale underlying these safe harbors, some scholars have gone further and argued that Congress should implement a *generalized* safe harbor rule that would replace the current patchwork of such rules and would apply to all contexts of information use and distribution online.[4] Yet the same type of safe harbor may not make sense in all creative and scientific contexts. And the very *patchwork* of rules governing the development and aggregation of online creativity may, due to the varied implementation of such rules in different creative contexts, be a more effective means of accounting for the diversity of motivational patterns in these different contexts than a generalized rule.

A patchwork of safe harbors, in other words, yields a variety of legal infrastructures that can be matched to differing structures of scientific and creative progress – and different motivational templates – on a more granular basis, in contrast to a uniform and universal safe harbor. Safe harbors are built upon a recognition that a solution appropriate to one industry structure (for instance, the protection of a person's rights in excludable and rivalrous physical goods as against a would-be thief of those goods) may not be appropriate to another (the protection of that person's rights in digital copies of goods as against a website provider that hosts others' potentially illicit copies of those goods). On an even more fine-grained level, context-specific safe harbors can be calibrated to enable greater protection for digital copies of some types of expensive goods that would not be designed but for the post-distribution ability to recoup the expenses necessary to the creation of such goods. Safe harbor diversity, in sum, enables laboratories of democracy as to how creative expression and reconfiguration will interact with the enforcement of legal protections on different areas of the Internet.

At the same time, the growth of the generative Internet places greater responsibility upon those who participate in and operate content and application platforms to develop internal mechanisms for deterring any harms to innovation, privacy,

---

[4] Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 102 (2007) (offering the safe harbor from liability for trademark infringement in 15 U.S.C. § 1114(2)(B)-(C) as a useful model for the creation of a "uniform safe harbor rule" which would replace the "confusing and illogical" patchwork of existing immunity rules).

and integrity of identity resulting from the under-enforcement of copyright, defamation, and other laws. The abstention from categorical line-drawing implied by safe harbors will yield a higher amount of harmful speech and innovation taking place online than would occur in the absence of safe harbors. If Internet users and application developers do not modulate these increased risks by developing reputation mechanisms and privacy protections, then it is likely that the developmental freedom associated with safe harbors will eventually be withdrawn by a legislative and judicial system that cannot tolerate these harms.[5] It is thus important to modulate these risks by encouraging users and application developers to build not just new forms of discourse but also protections against the extreme boundaries of such discourse.

For instance, users and developers can build reversion mechanisms into systems that will minimize the damage from instances of defamation or privacy invasions.[6] They can encourage conversational cooperation as opposed to atomistic trolling by endorsing internal reputation systems, such as the structured comment systems and mechanisms for associating users with rated profiles on Slashdot, Amazon, and CouchSurfing.[7] Finally, they can deputize watchdog groups in the mold of the Sunlight Foundation and StopBadware.org that catalogue harmful activities and facilitate a form of community policing of bad actors.

III. Internet Architecture

Safe harbors work hand in hand with other regulatory mechanisms to promote the free flow of information on the Internet. If CDA § 230(c) and DMCA § 512(c) promote the wide dispersal of information to and from diverse and antagonistic speakers by limiting the liability of the networks and platforms that carry such information, then loose structural interventions such as interconnection requirements and nondiscrimination rules preserve the kind of systemic network openness on which these and other unexpected types of user creativity can thrive.

Again, these regulatory mechanisms may conflict with the mechanisms of control typically exercised by managers of private infrastructure. But just as the best methods for promoting the progress of science and useful arts vary based on context of creative production and motivation, the best methods for promoting the development of network infrastructure vary based on the type of infrastructure at issue.

---

[5] *See* John Palfrey, "Dialogue [with Adam Thierer]: the future of online obscenity and social networks," Ars Technica, http://arstechnica.com/tech-policy/news/2009/03/a-friendly-exchange-about-the-future-of-online-liability.ars/2 (discussing a proposal to limit CDA 230 immunity and expand tort law-based negligence liability for interactive computer service providers).

[6] *See*, *e.g.*, Wikipedia, "Help: Reverting," http://en.wikipedia.org/wiki/Help:Reverting.

[7] CouchSurfing, a network for travelers and the hosts who provide their couches, not only provides detailed user profiles but also provides the opportunity for users to verify their name and address through means of a postcard sent to their home address in response to a small donation, CouchSurfing Verification, http://www.couchsurfing.org/verification.html, and to actively declare their trust for other members by "vouching" for them. CouchSurfing Vouching, http://www.couchsurfing.org/vouch.html ("When someone is vouched for, it signifies an elevated level of trust in the community. The only way to become vouched for is to be extremely trusted by someone who has been vouched for by three other members.").

A private command-and-control mechanism, whereby a single infrastructure owner is vested with the full ability to manage all other entities that wish to connect to that infrastructure, tends to work better when we only expect a single type of actor with a single-minded rational motivation to use the infrastructure in question. For instance, if users of a telephone system all simply want to use their telephone connections to make phone calls, or if users of a cable system all want to use the coaxial cables in their house solely to receive cable television signals, then a single network and a single manager may be best positioned to meet those singular needs and to respond rapidly and systemically when such needs are not being met. Analogously, if producers of certain scientific and artistic goods require a broad assurance of temporary monopolistic control over the products and expressions they create in order to justify the upfront investment of resources necessary to make these products and expressions in the first place, then a single system of exclusive rights-based incentives may ultimately yield the greatest amount of scientific and artistic innovation.

But where such actors or producers have diverse motivations and incentives (and in some cases are not even sure what use they wish to make of a given input until after having engaged in a series of experimental uses of that input), *or* where the optimization of a system for certain kinds of innovation frustrates the evolvability of that system and the growth of innovations that the designers of the original system could not have anticipated, then the creative model associated with centralized infrastructure management may fail to yield the desired high level of scientific and artistic progress and network development.

The Internet, which has been designed to promote interconnection and unforeseen use rather than a specific set of predictable uses, presents an example of this latter type of infrastructure. Through dividing a complex, interdependent network of networks into numerous encapsulated layers linked by common protocols, the architecture of the Internet has allowed participants at various layers to work on subparts of the larger network without needing to coordinate their work with participants at other layers. And it has continually erred on the side of wide distribution to and access by diverse participants.[8] No conscious decision by some grand union of network operators was every truly made, and yet the TCP/IP protocols were perpetuated through a variety of networks. Due to the openness of this protocol, the availability of standardized routers and Ethernet equipment, and the standardization of the protocol on most operating

[8] The 1980s saw a wide variety of burgeoning commercial, educational, and governmental networks on which users shared information with one another. However, the open Internet that we know today might never have come into existence were it not for the decision by those who were building out these networks to use the open TCP/IP protocol within their networks – a choice justified in part by the "interoperability, security, reliability, and survability" of TCP/IP. *See* Message from Michael Muuss <mike@brl-bmd> to Tcp-ip at Brl, "TCP/IP made Mandatory -- IEN 207." (noting in an internal Department of Defense memorandum that "[m]ilitary requirements for interoperability, security, reliability and survability are sufficiently pressing to have justified the development and adoption of TCP and IP in the absence of satisfactory nongovernment protocol standards"). This protocol, developed by Vint Cerf, was seen to "provide for 'host-to-host connectivity across network or subnetwork boundaries" in a way that other protocol standards could not. *Id*.

systems, the Internet grew rapidly in the late 1980s and 1990s as a wide variety of formerly isolated networks became interconnected.

The Internet is additionally built upon a modular design. According to the modularity-based approach to managing complex systems, the division of a complex, interdependent system into numerous encapsulated components "facilitate[s] specialization" and allows people to work on certain subparts of the system "in partial ignorance of what is going on in other modules."[9] This approach predicts that once a network is divided into modules or communities, such a network will yield higher benefits when the internal connections between particular nodes within any given module are dense (*e.g.*, when those who are working together on a task or a decision are highly dependent upon one another), but the system-wide connections between different modules are more sparse.[10] Modularity additionally allows a variety of experiments to take place in relatively independent laboratories within a given system, rather than concentrating all innovation resources in the quest for a singular solution.[11]

CONCLUSION

As the Department of Commerce seeks to reduce restrictions on the free flow of information on the Internet, then, it should seek to ensure maximal interconnection of networks and maximally diverse participation by users. These comments have focused on one way of implementing these goals: by promoting regulatory standards and safe harbors from liability that have allowed innovative intermediaries and users to flourish on the Internet.

---

[9] Henry Smith, *Intellectual Property as Property: Delineating Entitlements in Information*, 116 YALE L.J. 1742, 1761-62 (2007), *available at* http://yalelawjournal.org/images/pdfs/567.pdf.

[10] *See, e.g.*, Jörg Reichardt and Stefan Bornholdt, Statistical mechanics of community detection, PHYSICAL REVIEW E 74: 016110 (2006), *available at* http://dx.doi.org/10.1103%2FPhysRevE.74.016110; *see also* Mark S. Granovetter, *The Strength of Weak Ties*, 78-6 American Journal of Sociology 1360 (May 1973), *available at* http://www.stanford.edu/dept/soc/people/mgranovetter/documents/granstrengthweakties.pdf (formulating a theory of social networks based on the concept of "weak ties" which link together otherwise provincial and distant parts of a social system).

[11] *See* Carliss Y. Baldwin & Kim B. Clark, DESIGN RULES, VOL. 1: THE POWER OF MODULARITY (2000).