Safe Harbors and the National Information Infrastructure

NICHOLAS W. BRAMBLE*

In 1995, the Department of Commerce under President Clinton released a 267-page document arguing that strengthened intellectual property enforcement was necessary to ensure the population of the "national information infrastructure" with education, information, and entertainment products. Contrary to the predictions and recommendations of that paper, a very different set of laws emerged over the next decade and became dominant forces in the development of the U.S. information infrastructure. These provisions—section 512 of the Digital Millennium Copyright Act, section 230 of the Communications Decency Act, and the continued potency of Sony v. Universal*—generated a far more decentralized version of Clinton's global information society, one dominated not by commercial partnerships between network providers and content owners but instead by independent information intermediaries at the edges of the network.*

Other scholars have explored these safe harbors separately, but this Article fills a gap in the literature by looking at the collective, systematic impact of these laws upon the growth of the Internet. In so doing, this Article places § 512 and § 230 in the context of historical governmental attempts to shape the production and distribution of information. Many scholars and advocates have resisted this move, arguing instead that these laws, along with judicial decisions such as Sony v. Universal*, amount to the deregulation of the Internet and the creation of a lawless zone. But when these laws are considered together, a different picture begins to emerge: one where the government encourages the development of a "layer" of intermediaries situated between network providers (such as Comcast, AT&T, and Verizon) and content providers (such as Disney,* The New York Times*, and Viacom), and sets in place a legal framework that enables intermediaries to counteract the power of these network and content providers.*

Safe harbors, then, serve an important and unexamined regulatory function—a regulatory function that the government likely would have been unable to implement on its own (without the cooperation of intermediaries) due to jurisdictional, constitutional, technological, and political limitations on the government's power over Internet providers.

---

* Lecturer in Law, Yale Law School; Director, Law and Media Program, Information Society Project at Yale Law School; Visiting Research Collaborator, Princeton Center for Information Technology Policy. Thanks to Marvin Ammori, Jack Balkin, Yochai Benkler, Bryan Choi, Terry Fisher, Wendy Seltzer, and faculty and fellows associated with the Information Society Project at Yale Law School for advice and helpful comments on earlier drafts of this Article.

TABLE OF CONTENTS

INTRODUCTION

> It would be unfair—and set a dangerous precedent—to allow one class of distributors to self-determine their liability by refusing to take responsibility.
>
> —*Intellectual Property and the National Information Infrastructure*[1]

> [T]he time has come for the Internet to grow up and for Congress and the businesses that rely on the Internet to accept a mature scheme of regulation that limits the social costs of illegal Internet conduct in the most cost-effective manner.
>
> —*The Promise of Internet Intermediary Liability*[2]

> I think it is unrealistic to think we're going to continue to rely on the DMCA notice-and-takedown provision . . . . Anybody who is involved in providing services on the Internet would be expected to do some things.
>
> —Rep. Bob Goodlatte[3]

Dating back to President Clinton's Information Infrastructure Task Force and continuing through to the present day, scholars and governmental officials have called for network providers, search providers, and other Internet intermediaries to take a more active role in managing the flow of data on the Internet. These demands make a certain amount of intuitive sense. Intermediaries and online service providers are often the least cost avoiders, particularly when working in conjunction with rightsholders to root out infringing users.[4] They cannot hide behind the veils of anonymity that individual infringers sometimes use to avoid detection. They often oversee the activities of massive numbers of users. They have far deeper pockets than individual infringing users. They are seen to be more regulable because of deeper ties to government funding and greater susceptibility to regulatory chastisement. Finally, and perhaps most crucially, they are often capable of systematically tracking and expelling those users that engage in infringement, even if such tracking comes at the expense of user privacy.

---

1. BRUCE A. LEHMAN & RONALD H. BROWN, INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 122 (1995).

2. Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 250 (2005).

3. Gautham Nagesh, *Tech Groups Say Online Piracy Bill Would Create 'Nightmare' for Web and Social Media Firms*, HILLICON VALLEY (Oct. 31, 2011, 2:51 PM), http://thehill.com/blogs/hillicon-valley/technology/190781-tech-groups-say-online-piracy-bill-would-create-nightmare-for-web-and-social-media-firms (quoting Rep. Bob Goodlatte (R-Va.)).

4. *See* Mann & Belzley, *supra* note 2, at 240 (noting "an increase in the likelihood that it will be easy to identify specific intermediaries for large classes of transactions").

Yet two separate legal provisions have made it extremely unlikely that intermediaries will serve a more cooperative role as enforcement partners or economic middlemen of content and network providers. These provisions—the safe harbors from copyright liability in section 512 of the Digital Millennium Copyright Act ("DMCA")[5] and the immunity from defamation liability in section 230 of the Communications Decency Act ("CDA")[6]—helped create a legal ecosystem that insulated online intermediaries from the control of network providers, content providers, and to some extent the government itself.

By insulating Internet intermediaries from the control of these surrounding layers, these safe harbors have been the primary legal drivers of a fundamental historical shift in the availability of regulatory tools for the promotion of access to information and speech tools. When it was difficult for the average citizen to gain access to tools for speech and distribution of data, governmental officials (as well as scholars) sought to ensure that those who did have such access and control were tasked with the responsibility of distributing high-quality and high-value content.[7] But with the growth of the Internet came the potential for democratization of access to services for the production and distribution of speech. As the Organisation for Economic Co-operation and Development has noted, intermediaries "have brought unprecedented user and consumer empowerment through greater information, facilitating product and price comparisons and creating downward pressure on prices or, in the case of auction platforms, meeting supply and demand and creating new markets."[8]

As intermediaries build new platforms for data exchange and content distribution, the role of the government can shift—and has shifted—away from directly ensuring the presence of high-value information on speech platforms, and toward (a) maximizing the range and diversity of people that will be able to speak freely upon those platforms[9] and (b) preserving

5. 17 U.S.C. § 512 (2012).

6. 47 U.S.C. § 230 (2012).

7. *See, e.g.*, Red Lion Broad. Co., Inc. v. FCC, 395 U.S. 367 (1969); Cass Sunstein, *Free Speech Now*, 59 U. CHI. L. REV. 255, 296 (1992).

8. ORG. FOR ECON. CO-OPERATION & DEV., THE ECONOMIC AND SOCIAL ROLE OF INTERNET INTERMEDIARIES 4 (Apr. 2010). This Article follows the Organisation for Economic Co-operation and Development's general definition of online intermediaries as entities that "bring together or facilitate transactions between third parties on the Internet," *id.* at 9, but is particularly focused on those intermediaries that operate independently of Internet access providers and traditional content owners and licensors.

9. *See, e.g.*, A National Broadband Plan for Our Future, 76 Fed. Reg. 26,620 (May 9, 2011) (to be codified at 47 C.F.R. pt. 1).

the independence of these intermediary platforms from traditionally dominant industry incumbents.[10]

This shift alters traditional understandings of the purposes of the First Amendment as well as understandings of the proper interface between public regulators and private information intermediaries. Rather than needing to intervene directly in the operation of communications networks to ensure that broadcasters carry high-value speech to the public, governmental officials have used safe harbors to build an indirect regulatory framework. Essentially, this framework enables the development of a "layer" of Internet intermediaries that are capable of negotiating space for user speech against the potential constraints enacted by traditional content providers and network providers. The use of this layer-based framework as a form of regulation to promote access to speech infrastructure has sometimes been explicit, as in the case of section 230 of the CDA, but has more often been implicit, as in the case of section 512 of the DMCA and its subsequent judicial interpretations.[11]

Beyond the basic historical importance of articulating the parameters of this safe harbor-driven regulatory framework and situating it within First Amendment theory, the need to *defend* this regulatory framework has become particularly apparent over the last five years. Various court proceedings, international trade agreements, legislative proposals, and vertical mergers—including the recently proposed Stop Online Piracy Act[12] and Protect IP Act[13] as well as transactions between Comcast and NBCUniversal[14] and between Verizon and SpectrumCo[15]—threaten either to eliminate the Internet's "intermediary layer" or to transform it into a point of control through which network or content providers can limit or more finely manage user access to information.[16]

---

10. *See, e.g.*, Press Release, Dep't of Justice, Justice Department Allows Comcast-NBCU Joint Venture to Proceed with Conditions (Jan. 18, 2011), *available at* http://www.justice.gov/atr/public/press_releases/2011/266149.htm ("Comcast must relinquish its management rights in Hulu . . . . Without such a remedy, Comcast could, through its seats on Hulu's board of directors, interfere with the management of Hulu, and, in particular, the development of products that compete with Comcast's video service.").

11. *See infra* Part I.A–B.

12. Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011).

13. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong. (2011).

14. *See* Press Release, *supra* note 10.

15. Cellco Partnership Application, F.C.C. 12-95 (Aug. 23, 2012) (declaratory ruling); Cellco Partnership Application for Advanced Wireless Service Licenses, 27 F.C.C.R. 7169 (2012).

16. *See, e.g.*, Stop Online Piracy Act, H.R. 3261; Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968 (establishing a system for taking down websites that the U.S. Department of Justice determines to be "dedicated to infringing activities"); Combatting Online Infringements and Counterfeits Act, S. 3804, 111th Cong. (2010) (granting expanded powers to law enforcement officials to alter the configuration of domain names associated

The purpose of this Article, then, is to offer a clear picture of the multi-layered terrain on which legislators and regulators are acting when they threaten existing protections for intermediaries, and to tease out a submerged policy thread that can be used both to explain why safe harbors have been effective at promoting the development of user speech on the Internet and to figure out how best to preserve and build upon this regulatory success.

This Article proceeds in five Parts. Part I identifies the range of intermediary-driven strategies for promoting diverse forms of cultural development and intellectual activity that have evolved over the past two decades. Rather than leaving the growth of the Internet up to the cooperation of network providers such as AT&T and content providers such as Disney, Congress opted to set conditions for the growth of intermediaries on the Internet that could position themselves *between* these network and content providers. A wide variety of Internet intermediaries—search engines, blogging platforms, music- and video-sharing websites, social networks, discussion forum providers, and review aggregators—quickly began to populate this layer and to insert themselves into relationships between access providers and content providers. These intermediaries were generally able to negotiate between the competing interests of access providers and rightsholders in a way that redounded to the benefit of users. Part I summarizes the range of governmental interventions that drove the development of these networked intermediaries.

Part II contrasts limitations on intermediary liability with traditional governmental strategies for promoting wide public access to diverse and antagonistic sources of information. Scholars and legislators implemented these traditional strategies by asking courts or regulators to monitor the development of communications media and intervene where necessary to promote high-value speech and remove low-value speech. The goal of

---

with websites that are linked to infringing activities); Anti-Counterfeiting Trade Agreement, Dec. 3, 2010, *available at* http://www.ustr.gov/webfm_send/2417; *Application of Directive 2004-48-EC of the European Parliament and the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights*, SEC (2010) 1589 final (Dec. 12, 2010), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0779:FIN:EN:PDF (noting "intermediaries' favourable position to contribute to the prevention and termination of online infringements" and suggesting ways to "involve them more closely" with such efforts); Complaint for Declaratory & Injunctive Relief & Damages, Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 07-2103), 2007 WL 775611; *see also* Margot Kaminski, *The Origins and Potential Impact of the Anti-Counterfeiting Trade Agreement (ACTA)*, 34 YALE J. INT'L L. 247 (2009); Stanley Fish, *Anonymity and the Dark Side of the Internet*, N.Y. TIMES OPINIONATOR (Jan. 3, 2011), http://opinionator.blogs.nytimes.com/2011/01/03/anonymity-and-the-dark-side-of-the-internet ("The Internet and the real world, Leiter concludes, 'would both be better places' if Internet providers were held accountable for the scurrilous and harmful material they disseminate. How might that be managed? The answer given by the authors in [*The Offensive Internet*] involves the repeal or modification of Section 230 of the Communications Decency Act.").

these interventions was not necessarily to censor, but instead to promote diverse and antagonistic speech, rather than singular and harmonious speech. And the legal doctrine that evolved to support these interventions—in *Associated Press v. United States*,[17] *Red Lion Broadcasting v. FCC*,[18] and *Turner Broadcasting System v. FCC*[19]—rested upon a positive vision of the obligations of government under the First Amendment to structure forums for speech. This doctrine, insofar as it relied upon an understanding of the First Amendment as a mandate for the provision of access to speech forums, suffered setbacks toward the end of the twentieth century and the beginning of the twenty-first.

Part III situates safe harbors in the context of these traditional governmental interventions by analyzing two common accounts of the evolution of these laws. First, lawyers tend to portray safe harbors as a byproduct of the technological architecture of intermediary service providers, and courts have generally accepted these portrayals. But this mechanistic, post hoc portrayal of safe harbors and immunities from secondary liability can neither explain why such laws came into being in the first place, nor whether such laws should be maintained as intermediaries enhance their technological capacity to monitor user contributions or as industry incumbents seek a greater degree of vertical integration with intermediaries. Second, some scholars have gone further and considered how various safe harbors and immunities embody a legislative strategy to promote the democratic development of communications and distribution platforms. While this second explanation comes closer to a causative or normative explanation of limitations on secondary liability, it still suffers from inadequate consideration of how these laws—and the networked intermediaries they generate—destabilize the coordination dynamic between content providers and network providers and alter traditional governmental mechanisms for regulating these providers.

Neither of the accounts in Part III is sufficient, then, to explain the extent to which safe harbors have restructured the development of information and communications platforms, and reshuffled the roles of public and private regulators over these platforms. This lack of consideration of safe harbors and limitations on secondary liability as *forms of regulation* makes some degree of sense—the intervention strategies implemented by these laws, after all, do not imply an active role for courts or regulators in policing the development of content on

17. 326 U.S. 1 (1945).
18. 395 U.S. 367 (1969).
19. 512 U.S. 622 (1994).

the Internet. Still, more is going on here than the simple deregulation of the Internet.

Part IV considers the normative implications of safe harbors and analyzes whether we should consider this devolution of responsibility from governmental actors to online service providers to be a form of regulation. Networked intermediaries now exercise some of the same consumer protection functions that were formerly associated with regulators. Even though the law does not explicitly require intermediaries to act in the interest of users (and in fact typically shields them from liability for actions that end up being detrimental to specific users), user protection is in some sense the predicted result of the insertion of a new layer of intermediaries between network providers and traditional content providers. In the three-layer world made possible by safe harbors—with a new layer of information intermediaries inserted between existing layers of Internet access providers and content providers—the public has greater access to distributed communications platforms than they would have in a two-layer world composed solely of Internet access providers and content providers. Thus the creation and population of an "intermediary layer" essentially functions as a subterranean regulatory strategy to enhance public access to diverse sources of information on interconnected networks.

Yet Internet intermediaries do not act in a uniform way, nor do they always act in the public's interest. Safe harbors and immunities have distributed the basic functionality of the public domain over a wide variety of private information and communications providers, resulting in the radical decentralization of the public domain and the growth of a series of overlapping "private domains" or "commercial public domains," some of which are compatible with one another and some of which are not. Part V examines the tradeoffs that the government has made in asking private intermediaries to perform quasi-public regulatory functions. Over the past fifteen years, this distribution of responsibility for the maintenance of communications networks has been a productive way to implement the public's interest in access to information-sharing tools. But important questions remain regarding whether a more aggressive set of interventions will soon be needed to protect users and avoid fragmentation of the Internet, and whether the safe harbor-driven regulatory model provides a sustainable template for such interventions.

A good deal of scholarly attention has been paid to the mechanics of online immunities and safe harbors, to how these immunities and safe harbors evolved over the past fifteen years through judicial interpretation and private architectural design, and to how these legal provisions might either be tightened or loosened to promote different economic or social outcomes. Yet scholars have paid comparatively little attention to the

broader question of what the success of these safe harbors, considered together, means for the design of legal and regulatory architectures. This Article seeks to resolve that question and close a persistent gap in our understanding of the Internet's legal architecture.

I. A Brief Overview of Safe Harbors

The basic mechanisms underlying online safe harbors bear little resemblance to the operation of copyright laws, defamation laws, and even traditional offline safe harbors. Section 512 of the DMCA, section 230 of the CDA, and the opinion of the Supreme Court in *Sony v. Universal* are all part of a common thread of governmental decisions seeking to leave open sufficient room for the growth of technological and networked intermediaries.[20] These decisions—identified below under the common umbrella of "safe harbors"—have shielded intermediaries from secondary liability and thereby removed potential governmental and private constraints on the development of new Internet services.

While safe harbors shield a wide range of service providers from liability, including Internet access providers and other offerors of basic Internet connectivity services, this Article is primarily concerned with the impact of safe harbors upon the development of "information intermediaries" with which users directly interact on the Internet, rather than with the ISPs and caching providers that control the physical infrastructure through which users reach these intermediaries (or the copyright holders that license the content that users reach through intermediaries).[21] The following Part thus focuses on those specific

20. The proceedings at the FCC collected under the category of the "Computer Inquiries" have provided additional support for the growth of networked intermediaries, but because these proceedings do not operate under the same logic as safe harbors—that is, they do not carve out space for the growth of intermediaries by shielding those intermediaries from secondary liability—this Article does not analyze the Computer Inquiries in great detail. *See infra* text accompanying note 233.

21. Section 512 provides different levels of immunity to different types of intermediaries. *See* 17 U.S.C. § 512(a) (protecting telecommunications carriers for the temporary copies they make in the course of routing material from one user to another); *id.* § 512(b) (protecting providers that run proxy and caching servers that facilitate user access to content uploaded by other parties); *id.* § 512(c) (protecting service providers that store or host information uploaded by users); *id.* § 512(d) (protecting web directories and search engines that inadvertently link to infringing content). Other technological safe harbors addressed only in passing in this Article include safe harbors for digital audio recording devices, *id.* § 1001(3) (defining digital audio recording devices as devices "designed and marketed for the *primary purpose* of . . . making a digital audio copied recording for private use" (emphasis added)), and trademark law safe harbors protecting publishers against the inadvertent inclusion of trademarked material. *See infra* notes 141–143. Safe harbors analogous to the rule promulgated in *Sony v. Universal* have also absolved online intermediaries of immunity for infringement of trademarks by users of online services. *See, e.g.*, Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93, 103 (2d Cir. 2010) (holding that eBay was not contributorily liable for infringement of trademarks by counterfeiting vendors because eBay did not "culpably facilitat[e] the infringing conduct" of those vendors).

provisions of safe harbors that shield information intermediaries from liability.

A. Section 512(c) of the Digital Millennium Copyright Act: Conditional Immunity from Copyright Liability

In a complaint initially raised against YouTube's video sharing service in 2007, Viacom, a media company, alleged that YouTube had "harnessed technology to willfully infringe copyrights on a huge scale, depriving writers, composers and performers of the rewards they are owed for effort and innovation, reducing the incentives of America's creative industries, and profiting from the illegal conduct of others."[22] In its answer, YouTube responded that Viacom's copyright infringement claims were barred by "DMCA Safe Harbors in 17 U.S.C. § 512" and that the "DMCA balances the rights of copyright holders and the need to protect the internet as an important new form of communication."[23] The district court agreed with the reasoning of the defendants: YouTube responded quickly whenever it became aware of "specific and identifiable infringements of particular individual items," and to hold YouTube liable under a broader theory—for instance, conditioning liability on its failure to search out and take down infringing content on its service of which it was *not* specifically aware—would "contravene the structure and operation of the DMCA."[24] The court cited approvingly to the balance struck by Congress between the protection of copyright owners against massive piracy and the protection of service providers against massive copyright infringement liability.[25]

---

22. Complaint for Declaratory and Injunctive Relief and Damages ¶ 2, Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 07-2103), 2007 WL 775611.

23. Defendant's Answer and Demand for Jury Trial at 1, 10, *Viacom*, 718 F. Supp. 2d 514, 2007 WL 1724620. YouTube was later purchased by Google. With the *Viacom* litigation still ongoing, Google adopted a set of content filters that would "remove[] an offending video automatically if it matched some portion of a reference video submitted by a copyright owner." *See Viacom*, 718 F. Supp. 2d at 528 (describing YouTube's "Claim Your Content" system). Viacom continued to press its case against Google based on alleged infringement that had taken place up until the point at which Google offered its content-matching technology to all rightsholders. *See* Abigail Field, *Viacom vs. YouTube/Google: A Piracy Case in Their Own Words*, DailyFinance (Mar. 21, 2010, 1:45 PM), http://www.dailyfinance.com/2010/03/21/viacom-v-youtube-google-a-piracy-case-in-their-own-words.

24. *Viacom*, 718 F. Supp. 2d at 523. Last year, the court of appeals affirmed the district court's basic holding that the § 512(c) safe harbor "requires knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement." Viacom Int'l Inc. v. YouTube, Inc., 676 F.3d 19, 41 (2d Cir. 2012). However, as to section 512(c)(B), the court of appeals vacated the district court's interpretation that the "right and ability to control" required "item-specific knowledge" and instead referred the district court to examples where the right and ability to control infringement could be predicated upon a service provider's mere "exerti[on of] substantial influence on the activities of users." *Id.* at 38 (citing Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 937 (2005); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1173 (C.D. Cal. 2002)).

25. *Viacom*, 718 F. Supp. 2d at 519 (citing S. Rep. No. 105-190 (1998)).

Congress struck this "balance" only after providers of dialup Internet access services (such as America Online) and Internet platforms (such as Yahoo!) managed to delay passage of the DMCA by lobbying for the inclusion of the safe-harbor provisions in 17 U.S.C. § 512.[26] Congress was apparently convinced that it had to be attentive to the interests of these service providers in order to promote the build-out of the Internet's infrastructure.[27] Yet while Congress's goal in including safe-harbor provisions may have been to promote investments in the speed and capacity of the Internet, its statutory language—including its expansive definition of a service provider as a provider of "network access" or a provider of "online services"—was broad enough to allow courts to extend safe harbors to providers beyond those engaged in the provision of physical network infrastructure.[28]

The § 512(c) safe harbor states that a "service provider shall not be liable . . . for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider."[29] To qualify for this conditional immunity, the service provider in question must either be unaware that users have uploaded copyright-infringing material or else must act promptly to take down such material when notified of its presence.[30] In addition, if the service provider has the right and ability to control the presence of copyright-infringing material, then it must not

---

26. *See* JESSICA LITMAN, DIGITAL COPYRIGHT 143 (2006); Jessica Litman, *Real Copyright Reform*, 96 IOWA L. REV. 1, 6 (2010). Such provisions were included in the final version of the bill over the objections of proprietary software makers and entertainment conglomerates.

27. *See* S. REP. NO. 105-190, at 8 (1998) ("At the same time, without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet. . . . [B]y limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.").

28. 17 U.S.C. § 512(k)(1)(B) (2012).

29. *Id.* § 512(c)(1).

30. To be precise, a service provider can claim the benefits of the § 512(c) safe harbor only where that provider:

> (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material.

Id. § 512(c)(1)(A). Upon notification of an alleged infringement, the service provider must then "respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing." *Id.* § 512(c)(1)(C). *See* Yochai Benkler, *Wikileaks and the Protect-IP Act: A New Public-Private Threat to the Internet Commons*, 140 DAEDALUS 154, 159 (2011) ("Providers of caching, Web-hosting, and search engines and Web directories were required to have a procedure in place for receiving notices regarding specific offending materials, and for taking down those materials; but they were not required to search out such content themselves or to block entire sites.").

derive any financial benefit "directly attributable to the infringing activity," or else it will again fail to qualify for the immunity.[31]

The law does not give service providers an active duty to monitor and take down infringing content.[32] Instead, it effectively places this monitoring burden upon the rightsholder whose material is being stored on the service in question.[33] Website providers and Internet access providers alike have no duty to inspect the packets flowing over their platforms and networks.[34]

The logic of the balance struck by § 512 differs from the logic of the balance traditionally struck by copyright law. In the case of § 512, Congress sought to diminish the susceptibility of service providers to secondary copyright liability in order to promote the build-out of network infrastructure. In contrast, copyright law traditionally seeks to balance the exclusive control associated with the grant of the copyright entitlement (exercised under 17 U.S.C. § 106) with the interests of those who wish to have access to or to build upon the work protected by that entitlement (as represented by 17 U.S.C. §§ 107–22). There is an important difference between these two forms of logic: Copyright law sets up a pervasive regulatory system in which every interaction with a copyrighted work—and every enablement or facilitation of an interaction with a copyrighted work—is governed by a set of statutory balancing rules.[35] (In order to classify and regulate all possible creative interactions between users and rightsholders, copyright law requires roughly 200 pages of rules.) Section 512, on the other hand, does not seek to regulate individual interactions between users and rightsholders; instead, § 512 seeks to promote the growth of the network infrastructure on which these interactions take place. And the manner by which § 512 accomplishes this goal is by ensuring that independent service providers will not be deputized and vertically integrated as the predictive enforcement arms of rightsholders,[36] even where this lack of deputization results in wide berths where copyright entitlements are unlikely to be perfectly enforced.

---

31. 17 U.S.C. § 512(c)(1)(B).

32. *See id.* § 512; *see also* Viacom v. YouTube, 718 F. Supp. 2d 514, 524 ("The DMCA is explicit: it shall not be construed to condition 'safe harbor' protection on 'a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.'").

33. *See* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1113 (9th Cir. 2007) (declining to shift the burden of policing copyright infringement from the copyright owner to the service provider); *Viacom*, 718 F. Supp. 2d at 525 ("[I]f a service provider knows (from notice from the owner, or a 'red flag') of specific instances of infringement, the provider must promptly remove the infringing material. If not, the burden is on the owner to identify the infringement.").

34. 17 U.S.C. § 512(m) ("Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on . . . a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.").

35. *See, e.g.*, 17 U.S.C. § 107 (listing four factors of fair use analysis).

36. Section 512 "rein[s] in excesses and abuses as they happen, rather than preventing them from the outset." JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET 119 (2008).

By *refusing* to force intermediary service providers to act as preemptive enforcers of copyright law, legislators, perhaps indirectly, vastly diminished the threat of copyright infringement lawsuits to burgeoning forums for amateur creativity, and facilitated far more user activity than would likely have occurred in the absence of the § 512 safe harbor. The positive result of this regulatory cautiousness has been an abundance of online video and other forms of collaboratively produced media, much of it from individual contributors and little of it determined in advance or vetted by mainstream media producers (except insofar as these media producers contribute content that is later remixed, replied to, or parodied by outsiders).[37] YouTube and other video-sharing websites such as Vimeo and Veoh have thrived as locations for amateur creativity, even when the users supporting such sites have engaged, sometimes quite visibly, in questionably legal practices.[38] The U.S. Department of Commerce has stated that the services provided by Internet intermediaries such as Google, Facebook, YouTube, Twitter, and Flickr—sites that solicit the vast majority of their creative contributions from users—"are integral to the growth and vitality of the Internet because they allow widespread user participation with minimal upfront costs or technical resources."[39]

B. Section 230(c) of the Communications Decency Act: Wholesale Immunity from Defamation Liability

> Chris [Cox] and I hit on an idea that we felt would enable these new networks to protect their users without making them magnets for lawsuits. . . . It was our intention to protect the network effect from the smothering hand of government and litigation.[40]

A separate safe harbor shields service providers from the normal operation of defamation laws. The protection of "an individual's right

37. Preliminary research in 2009 by Michael Wesch suggested that approximately 80% of videos uploaded to YouTube were user-generated. *See* Michael Wesch, *YouTube Statistics*, Digital Ethnography at KSU (Aug. 13, 2008, 2:02 PM), http://ksudigg.wetpaint.com/page/YouTube+Statistics (classifying 80.3%of YouTube videos as "Unambiguously User-Generated (amateur)"); *see also, e.g.*, Kevin Allocca, '*Gangnam Style' Is Your International Hit of the Month*, http://youtube-trends.blogspot.jp/2012/08/gangnam-style-is-your-international-hit.html ("Naturally, we've already started to see lots of parodies/homages as well. In the past two weeks, nearly 1,000 videos have been posted with 'gangnam' (in English) in the title.").

38. *See, e.g.*, *Perfect 10*, 488 F.3d at 1114 (holding that the provision of services to websites named "illegal.net" and "stolencelebritypics.com" does not constitute awareness of circumstances from which infringing activity is apparent under § 512(c)(1)(A)(ii)).

39. Global Free Flow of Information on the Internet, 75 Fed. Reg. 60,068 (Sept. 29, 2010).

40. Nate Anderson, *Meet the Senator Blocking Big Content's Web Censorship Plan*, Ars Technica (Apr. 10, 2011, 6:00 PM), http://arstechnica.com/tech-policy/news/2011/04/meet-the-senator-blocking-big-contents-web-censorship-plan.ars (quoting Sen. Ron Wyden (D-Or.)) (second alteration in original).

[in] his own good name" is the goal of defamation law,[41] while securing dignity is a goal of personal privacy law.[42] Under the logic of defamation and privacy law, these goals are achieved by setting up exclusive individual entitlements; a violation of such laws gives the victim the right to go to court and seek a remedy for the loss of that entitlement. Traditionally, liability for violation of defamation law extended beyond the individuals who made a defamatory statement to forums that had the ability to publish and control the presence of defamatory statements.[43]

But the safe harbor in section 230 of the CDA, enacted in response to the *Stratton Oakmont v. Prodigy* decision,[44] states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[45] Congress's purpose in passing this law was to "promote the continued development of the Internet and other interactive computer services" and to "preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services."[46] To do so, it carved out a layer of online activity that it suggested would be "unfettered by Federal or State regulation," effectively shielding from liability those who collect and publish the speech generated by users within Internet communities.[47] With this provision, Congress sought to bolster its finding that the Internet was beginning to offer "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[48]

The result of § 230(c) was that "interactive computer service[s]"—which is to say, most communications networks and information-sharing platforms—would be treated under the law as *conduits* lacking responsibility for the actions of users, so long as these actions were not actively solicited or edited.[49] Under § 230, if an individual violates a

41. *See* Gertz v. Robert Welch, Inc., 418 U.S. 323, 341 (1974).

42. *See* Sorrell v. IMS Health, Inc., 131 S. Ct. 2652, 2672 (2011) ("The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure.").

43. *See* Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (finding Prodigy liable for the content of defamatory messages posted by users of its interactive service due to Prodigy's ability to control, screen, and edit content on this service); *see also* Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) (noting that the *Stratton Oakmont* court "held Prodigy to the strict liability standard normally applied to original publishers of defamatory statements").

44. *See Zeran*, 129 F.3d 327.

45. 47 U.S.C. § 230(c)(1) (2012).

46. *Id.* § 230(b)(1)–(2).

47. *Id.* § 230(b).

48. *Id.* § 230(a)(3)–(5) (listing Congressional findings).

49. The outer bound of liability for interactive computer services has likely been articulated by

statute, commits a tort, or breaks a contract while using one of these interactive consumer services, then the victim of this violation retains the right to sue the individual violator. But this victim "can no more sue the host of the web site, or the provider of the email service, than he could sue the postal service for carrying a defamatory book or newspaper, or sue a library for lending such a book out."[50] Even where an interactive computer service has engaged in editing or censorship of user-contributed expression, § 230(c)(2) contains a good-faith exception that protects such a service from accruing responsibility and liability for shaping this expression.[51]

Section 230(c) applies to a wider range of providers of interactive computer services than was likely contemplated at the time of the law's passage.[52] Courts have interpreted the § 230 immunity to apply even where service providers have "knowledge of defamatory content on their services."[53] Broad and strong immunity has allowed entities like eBay, Amazon, Craigslist, YouTube, and Facebook to create unique social sites that encourage the sharing and development of information and speech by their users.[54] A wide range of search engines (e.g., Google and Bing),

---

the Ninth Circuit in its controversial split decision holding a website called *Roommates.com* liable for content posted by users. *See* Fair Hous. Council, San Fernando v. Roommates.com, 521 F. 3d 1157, 1176 (9th Cir. 2008) (McKeown, J., dissenting) ("By exposing every interactive service provider to liability for sorting, searching, and utilizing the all too familiar drop-down menus, the majority has dramatically altered the landscape of Internet liability.").

50. *See* Paul Alan Levy, *Stanley Fish Leads the Charge Against Immunity for Internet Hosts—But Ignores the Costs*, CONSUMER LAW & POLICY BLOG (Jan. 8, 2011), http://pubcit.typepad.com/clpblog/2011/01/stanley-fish-leads-the-charge-against-immunity-for-internet-hosts-but-ignores-the-costs.html (defending anonymous speech on grounds including protection of whistleblowers who do "not want to take the risk of obloquy . . . or of economic retaliation").

51. Section 230(c)(2) provides that "[n]o provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."

52. *See* Mark Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 103 (2007) ("[Section 230(c)] has been interpreted quite broadly to apply to any form of Internet intermediary, including employers or other companies who are not in the business of providing Internet access and even to individuals who post the content of another." (footnote omitted)). Section 230(c) has created the conditions for the growth of a variety of websites not prevalent in 1996, including "blogs, consumer criticism ('gripe') sites, political discussion sites, and countless other sites such as SexSearch.com." *See* Brief of Amici Curiae Center for Democracy & Technology and Electronic Frontier Foundation Supporting Appellees and Urging Affirmance at 15, John Doe v. SexSearch.com, 551 F.3d 412 (6th Cir. 2008) (No. 07-4182) [hereinafter CDT Sexsearch Brief].

53. Zeran v. Am. Online, 129 F.3d 327, 333 (4th Cir. 1997) (reasoning that any form of notice-based liability would "reinforce[] service providers' incentives to restrict speech and abstain from self-regulation"). The foundational judicial interpretation of § 230 supplies a number of architectural and speech-based rationales for § 230 beyond those listed in the statute—the text of which primarily consists of aspirational statements about the Internet and suggestions for the private development of tools for filtering and blocking objectionable content. *Compare id. with* CDA, 47 U.S.C. § 230(a), (b).

54. *See* Jack Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 436

blogging platforms (e.g., Tumblr and Facebook), video-sharing websites (e.g., YouTube and Vimeo), social networks (e.g., Facebook and Twitter), discussion forums (e.g., Reddit and Metafilter), commerce websites (e.g., Craigslist and Etsy), and consumer review platforms (e.g., Yelp and TripAdvisor) rely on § 230(c). Without this provision, those who offered a communications platform to outside parties would assume the status of "publisher" or "speaker" of information generated by those outside parties, and would face the attendant liability that comes with being a publisher or speaker of tortious or contract-violating communications.[55] Providers of websites and other "interactive computer services" would consequently need to assume a higher degree of responsibility over the user-generated data they solicit and host, and the likely result would be platforms that hosted and solicited far less of that data.[56]

Notably, the broader intention of Congress in enacting the Communications Decency Act was actually to *reign in* indecent and obscene material on the Internet.[57] Yet those provisions of the law concerning indecency were found to be unconstitutional restrictions on freedom of speech in violation of the First Amendment,[58] while the exception to the unconstitutional provisions survives to this day.

C. THE *SONY V. UNIVERSAL* JUDICIAL SAFE HARBOR: CAPABLE OF SUBSTANTIAL NON-INFRINGING USES

Courts, too, have taken an active—if not entirely premeditated—role in creating preconditions of creative abundance by allowing independent technological intermediaries to develop around the edges of copyright law. Although the following safe harbor does not apply directly to the information intermediaries and online service providers that are the subject of this Article, it offers an instructive parallel from the development of the consumer electronics industry.

(2008) ("Without something like the § 230 immunity, it would be very risky to create social software that allows others to blog or publish, much less create a social networking site. Indeed, search engine companies like Google, which publish snippets of other people's sites to help you find them, or advertising sites like Craigslist, which act as community bulletin boards, would be in serious jeopardy, not to mention sites like Amazon.com which encourage customer reviews and commentary."); *see also* YOCHAI BENKLER, THE WEALTH OF NETWORKS 92 (2006) (describing how web-based organizational tools have enabled "behaviors and motivation patterns familiar to us from social relations . . . [to] become effective beyond the domains of building social relations . . . and fulfilling our emotional and psychological needs").

55. *See* CDT Sexsearch Brief, *supra* note 52, at 6 ("Inevitably, when millions of people are speaking, some of that speech will be objectionable.").

56. *Id.* at 15.

57. *See* Communications Decency Act of 1996, Title V § 502, Pub. L. No. 104-104, 110 Stat. 133 (1996) (imposing criminal sanctions on anyone who knowingly uses computer networks to display offensive material to underage users).

58. Reno v. ACLU, 521 U.S. 844, 849 (1997).

In *Sony v. Universal*, after finding that "[c]opyright protection . . . . has never accorded the copyright owner complete control over all possible uses of his work,"[59] the Supreme Court held that because Sony's videotape recorder was capable of substantial noninfringing uses—e.g., authorized time-shifting—the sale of this recorder did not constitute copyright infringement, despite its capacity for facilitating such infringement.[60] By articulating a test for secondary infringement that hinged upon whether a given technological device or piece of software was "*capable* of substantial non-infringing uses,"[61] the Supreme Court further divested copyright law of some of its exclusionary character in order that it might not stand in the way of the growth of new technological intermediaries.[62] This type of judicial solution, particularly insofar as it entails an explicit legal carveout for technological and organizational tools that would not exist under traditional legal regimes, closely mirrors the legislative justifications for safe harbors developed above. Whether or not it is a true safe harbor, the *Sony* standard manages to focus judicial attention on the *capabilities* of a technology rather than its current applications.

Emphasizing the first word in the "capable of substantial non-infringing uses" standard, as courts following the *Sony* standard have done,[63] portends a shift in judicial examination away from the initially apparent character of a given invention or service (except insofar as it is readily discernible that an original creator explicitly designed that service with copyright-infringing motives and interests),[64] and toward examination of how downstream users and listeners of a given invention, or a given service, will use and enhance that invention or that service to fit

59. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 432 (1984).

60. *Id.* at 456.

61. *Id.* (emphasis added).

62. For this reason, some commentators have argued that the *Sony* judgment functions as "a form of judicial safe harbor" for those seeking to develop innovative technologies that challenge rightsholders' entitlements under copyright law to maintain control over reproduction and distribution of their copyrighted works. *See, e.g.*, Michael J. Madison et al., *Constructing Commons in the Cultural Environment*, 95 CORNELL L. REV. 657, 702 (2010); *see also* Pamela Samuelson, *The Generativity of* Sony v. Universal*: The Intellectual Property Legacy of Justice Stevens*, 74 FORDHAM L. REV. 1831, 1850 (2006) ("Without the safe harbor [*Sony v. Universal*] provides, tape recorders, photocopiers, CD burners, CD ripping software, iPods, and MP3 players, and a host of other technologies that facilitate private or personal use copying might have never become widely available.").

63. *See, e.g.*, MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 939 n.12 (2005) (noting that liability for inducement of copyright infringement cannot be "merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses").

64. *See id.* at 934, 937 (holding that an "actual purpose to cause infringing use" may be sufficient to subject a technology distributor to inducement liability but rejecting the notion that "mere knowledge of infringing potential or of actual infringing uses" may give rise to such liability).

unexpected needs.[65] As with the legislative safe harbors described above, this shift in emphasis captures the basic uncertainty associated with technological development and underscores the distributed, experimental character of such development.

In conclusion, online safe harbors offer broad exemptions from the operation of copyright and defamation laws. Unlike traditional limitations and exceptions within copyright law, which tend to offer highly specific exemptions from otherwise dominant laws and rights,[66] § 512, § 230, and *Sony v. Universal* have been interpreted by courts to grant immunity (or conditional immunity) to a wide range of activities engaged in by a wide range of intermediaries. The framers of legislative immunities and safe harbors such as section 512 of the DMCA and section 230 of the CDA sought to craft a new set of legal mechanisms to promote the public's interest in "diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[67] To a remarkable extent, these predictions came true. These safe harbors, coupled with longstanding regulatory standards limiting the ability of owners of telecommunications networks to control either the devices attached to those networks or the software and applications accessed via those networks,[68] resulted in an explosion of the amount of user-generated information and communications tools available on the Internet. The following Part will examine how safe harbors fit within the context of historical governmental attempts to shape the production and distribution of information.

II. Problems with Prior Attempts to Shape the Development of Markets for Speech and Culture

By permitting a new group of intermediaries to solicit, aggregate, and distribute content generated by users without thereby becoming liable for that content, § 512(c) and § 230(c) promoted the wide dispersal of information to and *from* diverse and antagonistic speakers in a far more efficient and effective way than previous laws, regulations, and judicial doctrines—and the previous technologies created by those

65. Academic literature on innovation provides support for this shift in emphasis. *See, e.g.*, Carliss Y. Baldwin & Eric von Hippel, *Modeling a Paradigm Shift: From Producer Innovation to User and Open Collaborative Innovation* (MIT Sloan Sch. of Mgmt., Working Paper No. 4764-09, 2010), *available at* http://ssrn.com/abstract=1502864.

66. *See generally* Jessica D. Litman, *Copyright, Compromise, and Legislative History*, 72 Cornell L. Rev. 857 (1987).

67. CDA, 47 U.S.C. § 230(a) (2012).

68. *See, e.g.*, Internet over Cable Declaratory Ruling, Appropriate Regulatory Treatment for Broadband Access to the Internet over Cable Facilities, CS Docket No. 02-52, Policy Statement, 20 FCC Rcd. 14986 (2005) (open Internet policy statement of Michael Powell); *In re* Carterfone, 13 F.C.C.2d 420 (1968).

laws—could have contemplated.[69] The amount of political, cultural, and intellectual information shared on the Internet soared from 1996 to 2012.[70] Together, safe harbors and regulatory standards transformed the Internet from a one-to-many digital space (in which it was supposed that the bulk of new "education, information and entertainment products" would be distributed via agreements between network providers and traditional media providers)[71] into a fully networked many-to-many space.[72] Furthermore, as safe harbors gave rise to a layer of online intermediaries that functioned independently of the owners of underlying network infrastructure, new intermediaries—including Spotify,[73] Netflix,[74] Hulu,[75] and other platforms unlikely to invoke the protections of § 512 and § 230—joined this layer and marketed their independent aggregation and distribution services to traditional content providers eager to build new platforms for the distribution of licensed music and video. Through this process, the diversity of licensed and unlicensed information on the Internet continued to grow.

At the same time, the laws and regulations supporting the growth of this layer of online intermediaries—and the new globally networked communications platform that arose around such intermediaries—also made it extremely difficult for governmental or private entities to impose more traditional regulatory frameworks upon the "higher" content or "lower" physical layers of that communications platform. Instead, lawmakers found that much of the action was taking place on the

---

69. *See infra* Part V.A.

70. Google, for instance, estimates that approximately two billion YouTube videos are viewed each day. *See* Google, Comments to Department of Commerce: Inquiry on Copyright Policy, Creativity, and Innovation in the Internet Economy, Docket No. 100910448-0448-01 (2011), *available at* http://www.ntia.doc.gov/comments/100910448-0448-01/comment.cfm?e=6BDC88CD-BD11-4506-9196-220C54FBBB87.

71. *See* LEHMAN & BROWN, *supra* note 1, at 10, 177 ("[C]ontent providers must have secure and reliable means for delivering information products and services to consumers. This means that content providers must be confident that the systems developed to distribute these works will be secure and that works placed on these systems will remain authentic and unaltered. If content providers cannot be assured that they will be able to realize a commercial gain from the sale and use of their products using the NII, they will have little incentive to use it.").

72. A networked space is one that enables "large numbers of people to broadcast and publish to audiences around the world, to be speakers as well as audiences, to be active producers of information content, not just recipients or consumers." Balkin, *supra* note 54, at 440.

73. *See* David Meyer, *Virgin Media: Spotify Deal Will Bring Down Piracy*, ZDNET UK (July 6, 2011, 7:57 AM), http://www.zdnet.com/virgin-media-spotify-deal-will-bring-down-piracy-3040093328.

74. *See* Brooks Barnes & Brian Stelter, *Netflix Secures Streaming Deal with Dreamworks*, N.Y. TIMES (Sept. 25, 2011), http://www.nytimes.com/2011/09/26/business/media/netflix-secures-streaming-deal-with-dreamworks.html.

75. *See More About Hulu*, HULU, http://www.hulu.com/about/media_faq#relationship (last visited Dec. 7, 2012) ("Hulu brings together a large selection of videos from more than 410 content companies . . . .").

comparatively unregulated intermediary layer between these content and physical layers.

As a result, the growth of the Internet presents policymakers with another more fundamental set of challenges. The previous Part examined the impact of safe harbors upon the operation of copyright and defamation laws. The following Part examines what safe harbors do to our understanding of traditional justifications for governmental attempts to ensure access to high-value information. With the rise of the Internet, driven by safe harbors, comes a radical shift in the government's ability to promote wide public access to tools for viewing, producing, and distributing information. But with that shift comes an accompanying *diminishment* of the government's ability to ensure and accredit the value of that data.

The following Part asks, then, whether the basic mechanisms associated with safe harbors—non-intervention, immunity, and the preservation of independence from traditional distribution networks—can serve the goals of the First Amendment as set forth by theorists such as Robert Post, Cass Sunstein, Yochai Benkler, and Lillian BeVier, or whether some more aggressive set of interventions may be needed.

A. Promoting High-Value Speech?

What role, if any, should the government play in promoting a functioning marketplace for ideas, incentivizing innovative uses and methods for organizing those ideas, and supporting investment in the basic infrastructure underlying this communications platform?[76]

The difficulty in answering these kinds of questions is that it quickly forces one back upon first principles. How are we to measure the development of a market for *ideas*? From what sort of baseline does one weigh the "costs" of Internet speech against its benefits and conclude that some measure of additional intervention is necessary? Does innovation within this marketplace primarily depend upon investing in or allocating control to those who provide the network's core physical layers, or should regulations and resources be devoted to ensuring that application developers are free to experiment at the ends of networks without obtaining consent from network providers? What is to be done when a marketplace of ideas exhibits symptoms of market failure? How should signals be structured to encourage speakers and managers of speech infrastructure to account for external costs generated by their actions in this marketplace? Does this market function most effectively

76. *See generally* Robert Post, Democracy, Expertise, Academic Freedom: A First Amendment Jurisprudence for the Modern State (2012); *see also* Lillian R. BeVier, *Can Freedom of Speech Bear the Twenty-First Century's Weight?*, 36 Pepp. L. Rev. 415 (2009).

when it is most liquid? Or does excessive liquidity of user speech and user information lead to unexpected harms, such as overload of unorganized and unaccredited information or the increasing availability and searchability of private or defamatory information?

The core problem here, identified nearly two decades ago by Sunstein, is that "we do not know what a well-functioning marketplace of ideas would look like."[77] Accordingly, we are unable to specify the preconditions of a market for free expression.[78] As opposed to an economic marketplace, where such preconditions are fairly well-established (if also heavily contested), the concept of an *expressive* marketplace forces policymakers to consider anew just what signals and patterns of interaction need to be in place and what goals need to be accomplished in order for this "market" to succeed.[79]

Sunstein, after considering these questions, concludes that it is largely up to courts to ensure a vibrant marketplace of ideas by granting more First Amendment protection to forms of speech connected to political deliberation and less protection to advertisements, libel of celebrities, pornography, technological data, and other forms of "low-value speech."[80] Sunstein's substantive conclusion mirrors Alexander Meiklejohn's argument that "what is important in a system of free expression is not that everyone gets to speak but that 'everything worth saying shall be said.'"[81] In short, the presence of high-value speech is a more important value than the presence of diverse speakers, and both governmental and judicial interventions in the marketplace for speech should seek to promote this First Amendment value.[82]

Sunstein's answer seems incomplete today, both in the role it assumes courts will play in promoting high-value speech[83] and in the assumptions it makes about the structure of the media environment.[84]

---

77. Sunstein, *supra* note 7, at 296.

78. *See id. But see* JULIE COHEN, CONFIGURING THE NETWORKED SELF 9 (2011) ("The environment within which artistic and intellectual culture emerges and evolves isn't a market, though it contains markets. It is a social entity, generated by patterns of human and institutional interaction. . . . [W]e can't deploy economic laws to generate scientifically determinate prescriptions for their optimal form.").

79. *See* Madison et al., *supra* note 62, at 669 ("[L]egal facilitation of innovation and creative production is not—and cannot—be confined to a simple set of property rules to incentivize individual innovative and creative efforts.").

80. Sunstein, *supra* note 7, at 301–06.

81. Balkin, *supra* note 54, at 440 (quoting ALEXANDER MEIKLEJOHN, POLITICAL FREEDOM: THE CONSTITUTIONAL POWERS OF THE PEOPLE 26 (1960)).

82. *See generally* Jack M. Balkin, *Media Access: A Question of Design*, 76 GEO. WASH. L. REV. 933 (2008); Jerome A. Barron, *Access to the Press—A New First Amendment Right*, 80 HARV. L. REV. 1641 (1967).

83. *Cf.* Arizona Free Enter. Club's Freedom Club PAC v. Bennett, 131 S. Ct. 2806, 2825 (2011) ("We have repeatedly rejected the argument that the government has a compelling state interest in 'leveling the playing field' that can justify undue burdens on political speech.").

84. *See infra* Part IV.C.

Limitations on secondary liability, in conjunction with the development of open and abundant network interconnectivity, have undermined the technological and jurisdictional basis of a series of traditional public protections for communication and innovation.[85] For example, it is hard to imagine an ongoing role for courts or Congress in monitoring the content of Internet speech after *Reno v. ACLU*,[86] which struck down content controls in the face of the Internet's "vast democratic forums" which lacked either a "history of extensive Government regulation" or the characteristics of scarcity and invasiveness associated with earlier media platforms.[87] Other technological and policy levers that have begun to fall by the wayside include: copyright-based tools granting creators full control over the dissemination of their works; media access tools such as the fairness doctrine and rights of reply;[88] rules limiting children's exposure to obscenity and pornography;[89] and structural provisions mandating a certain level of local ownership of media distributors.[90]

Beyond legal difficulties, speech monitors would also face technological difficulties in assessing the layers of communications tools that speech passes through as it moves from speaker to device to conduit to audience. Given that Sunstein gave this answer prior to the rise of the modern Internet, during an era in which broadcast television and radio were still dominant (along with cable, the regulation of which is subject to intermediate but not strict scrutiny),[91] it is not surprising that he did not develop a careful empirical plan for analyzing the development of a marketplace of ideas or for comparing the variety of potential private and public legal and communications tools that now might be used to build this marketplace. Yet it *is* surprising that no one since Sunstein has devoted time to developing such a plan.[92]

---

85. *See, e.g.*, Christopher S. Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience*, 78 GEO. WASH. L. REV. 697, 747 (2010) ("Whatever the continuing validity of the bottleneck rationale with respect to cable television, it almost certainly has no applicability to the Internet.").

86. *See* Reno v. ACLU, 521 U.S. 844, 885 (applying strict scrutiny to a law designed to shield children from unsuitable speech on the Internet).

87. *Id.* at 868–69 (distinguishing regulations of content on the Internet from regulations of content on media to which lesser standards of constitutional scrutiny have applied). In *Reno*, the Court declined to apply standards for limited First Amendment scrutiny of media regulations articulated in earlier broadcasting cases such as *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367, 399–400 (1969), cable television cases such as *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622, 637–38 (1994), and satellite broadcasting cases such as *Sable Communications of California, Inc. v. FCC*, 492 U.S. 115, 128 (1989).

88. Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 256 (1974).

89. Ashcroft v. ACLU, 542 U.S. 656, 661 (2004) (affirming on First Amendment grounds a decision to uphold a preliminary injunction against the enforcement of the Child Online Protection Act).

90. *See infra* Part IV.

91. *Turner Broad. Sys.*, 512 U.S. at 637.

92. Sunstein later advanced a separate concern that filters on the Internet will enable users to fully separate themselves from facts and narratives that they do not wish to hear or read. *See* CASS

B. Promoting Diverse and Antagonistic Sources of Information?

In a recent article, Derek Bambauer laments that those who advocate governmental intervention in shaping information environments fail to offer a methodology to "evaluate the state of on-line information" or "to measure whether the government has achieved progress."[93] But the problem with measuring the "progress" of information and cultural environments is that it is difficult to determine the normative or descriptive goal with respect to which such measurements should be made.[94] Other environments—and other markets—can be evaluated based on objective scientific or economic principles, but when the goal of evaluation is to assess cultural values and cultural harms, information measurement may be hopelessly subjective.[95] Culture, as Julie Cohen has observed, is marked by "patterns of human and institutional interaction," and while some of these patterns may be amenable to principles of economic measurement, it will be difficult to use those same principles "to generate scientifically determinate prescriptions" for the "optimal form" of culture.[96]

Rather than formulate a detailed plan for achieving an ideal pattern of cultural action and empirical metrics for analyzing progress toward that pattern, then, many instead retreat into a subjective, almost intuitive preference for "diverse and antagonistic" forms of interaction, on the one hand,[97] or a similarly intuitive antipathy toward any structural limitation on fully liquid and unregulated marketplaces, on the other hand.[98] In either case, the prevailing definition of informational and cultural progress approaches Justice Potter Stewart's definition of pornography: We know it when we see it.[99]

Sunstein, Republic.com 2.0 (2007). But Sunstein's solutions in that book focus largely on broadcasters. *See id.*

93. Derek Bambauer, *Orwell's Armchair*, 79 U. Chi. L. Rev. 863, 941 (2012).

94. Cohen, *supra note* 78 at 3–5 ("[B]oth property and speech arguments about digital architectures share some peculiar characteristics, beginning with the confident assumption that one or the other discourse can be made to generate definitive rules for resolving disputes about how much control is too much.").

95. *See* Susan Crawford, *The Communications Crisis in America*, 5 Harv. L. & Pol'y. Rev. 245, 260 (2011) ("Cultural policy is much more difficult to address. . . . Can the un-measured and perhaps un-measurable effects of consolidation and control—the opposite of diversity—have an impact even if they can't be counted?").

96. Cohen, *supra* note 78, at 9.

97. *See id.* at 8 ("Cultural environments have attributes and tendencies, but they are far less predictable, and their health is a matter of opinion.").

98. *See, e.g.*, Citizens United v. FEC, 558 U.S. 310, 130 S. Ct. 876, 906, 907 (2010) ("*Austin* interferes with the 'open marketplace' of ideas protected by the First Amendment. . . . The censorship we now confront is vast in its reach. The Government has 'muffle[d] the voices that best represent the most significant segments of the economy.'").

99. Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

For instance, consider the following attempt to set forth a normative claim with respect to which progress can be measured: An information environment that promotes wide patterns of interaction with diverse institutions will produce a more democratically competent and accountable culture than an information environment that promotes a narrower range of interaction with more monolithic institutions. This general observation, emerging from the Supreme Court's opinion in *Associated Press v. United States*,[100] may ring true on an abstract level, but it is of little help in assessing how well current and proposed policy interventions actually promote a more variegated and less concentrated culture.[101] For example, the rise of cable television can certainly be read as the opening up of a world of information sources that previously had been dominated by three broadcasters,[102] but others might instead see cable television as an attack on traditional notions of a common television culture, as a distraction from richer or more interactive sources of information that are not subject to control by cable operators, as an enabler of a world of "echo chambers" and "information cocoons,"[103] or as one more contribution to an already vast wasteland.[104] Nor will so general an observation be of much help at the micro level in predicting, for instance, whether an increase in the length of a copyright term will promote or inhibit wide patterns of interaction, or whether allowing Internet access providers to implement two-sided pricing of Internet traffic will generate clearer market signals as to where information providers should increase or reduce investment.

There are two possible responses when faced with this critique of the project of defining high-value speech. The first is to try harder to come up with a better empirical framework in which to assess the development of information flow and culture. From a technological

---

100. Associated Press v. United States, 326 U.S. 1, 20 (1945).

101. *See* Daniel E. Ho & Kevin M. Quinn, *Viewpoint Diversity and Media Consolidation: An Empirical Study*, 61 STAN. L. REV. 781, 860 (2009) ("Neither convergence nor divergence inexorably follows from consolidation."). *But see* Marvin Ammori, *First Amendment Architecture*, 2012 WIS. L. REV. 1, 45 (citing literature debating this empirical point and noting that "Judge Learned Hand has declared that we have 'staked' our nation on this basic tenet" of dissemination of information from diverse and antagonistic sources). This broader debate between uniform and distributed policy solutions can be traced back to the founding of the American republic. Wrote one anti-federalist: "In a republic, the manners, sentiments, and interests of the people should be similar. If this be not the case, there will be a constant clashing of opinions; and the representatives of one part will be continually striving against those of the other." BRUTUS, THE COMPLETE ANTIFEDERALIST 369 (1980). To this, Alexander Hamilton responded that "the jarring of parties" will "often promote deliberation." THE FEDERALIST No. 70 (Alexander Hamilton).

102. *See* TIM WU, THE MASTER SWITCH 212 (2010).

103. SUNSTEIN, *supra note* 92, at 44.

104. *See* Newton Minow, Speech to National Association of Broadcasters (May 9, 1961), *available at* http://www.americanrhetoric.com/speeches/newtonminow.htm.

standpoint, Measurement Labs, for instance, is a rigorous attempt to map out constraints on data flow at various layers of communications networks.[105] From a legal empirical standpoint, Christopher Sprigman, Kal Raustiala, Christopher Buccafusco, and others have done extensive empirical research in examining the theoretical assumptions underpinning copyright and patent incentives and relating those assumptions to models of cultural development.[106] From a more normative perspective, Bambauer suggests trying harder to define what counts as good or bad suppression of speech by developing a "process-based methodology" to evaluate whether a given censorship decision is based upon direct, democratic, and transparent procedures (in which case it is legitimate) or instead upon indirect, opaque, and "soft" procedures (in which case it is illegitimate).[107] And from a more critical standpoint, Cohen has recommended looking to fields such as cultural anthropology to come up with better "descriptive and normative accounts of culture itself," and then applying those accounts—rather than the thin methodological account of liberal individualism that she sees as underlying the free culture and access to knowledge movements—to assess the value of culture.[108]

The second response to the difficulty of defining high-value speech, however, is to temporarily abandon these descriptive and normative attempts to define ideal patterns of interaction, and instead to work on developing frameworks in which distant legislators and regulators *need not worry* about designing the perfect set of incentives for the production of high-value information.[109] Under this alternative programmatic vision of governmental intervention into communications networks, officials would be freed to focus on the project of building architectures for the networked distribution of data, and would no longer need to expend resources on the considerably more difficult problem of "set[ting] and enforc[ing] the terms and conditions under which . . . works are made available in the Network Information Infrastructure environment."[110] This is, indeed, one reading of

105. *See About Measurement Lab*, MLAB, http://www.measurementlab.net/content/about-measurement-lab (last visited Dec. 7, 2012) ("The goal of M-Lab is to advance network research and empower the public with useful information about their broadband connections.").

106. *See, e.g.*, Christopher Buccafusco & Christopher Sprigman, *Valuing Intellectual Property: An Experiment*, 96 CORNELL L. REV. 1, 6–15 (2010) (analyzing the impact of the endowment effect upon authors' versus audiences' valuations of copyrighted works). If this social science research is correct, and "small changes in the context of a decision can greatly affect the extent to which people value a particular good or property right," *id.* at 7, then the situational findings in these works may cut against the project of discovering generalized rules that apply to all creative domains in more or less equal measure.

107. *See* Bambauer, *supra* note 93, at 873.

108. COHEN, *supra* note 78, at 5.

109. *See* Mark MacCarthy, What Internet Intermediaries Are Doing About Liability and Why It Matters 42 (Oct. 2009) (unpublished draft), *available at* http://works.bepress.com/mark_maccarthy/1.

110. LEHMAN & BROWN, *supra* note 1, at 10.

the Supreme Court's opinion in *Associated Press v. United States*: Part of the project of promoting "the widest possible dissemination of information from diverse and antagonistic sources" entails *refraining* from making certain judgments as to what sorts of information should and should not be disseminated and taking certain actions as a result.[111] Instead, achieving this democratic ideal requires building networks in which diverse parties are capable of receiving and generating information, and then intervening in those networks only where some party has put up a roadblock that inhibits the generation, distribution, security, or clear reception of information.

Under this reading of *Associated Press v. United States*, the single most important thing that officials can do to carry out the purposes of the First Amendment is to set up and enforce legal architectures in which information moves effectively from person to person and from institution to institution without network operators setting up private tollbooths that favor or disfavor certain sources of information.[112] The government has a duty, under this theory, to facilitate the spread of knowledge through the development of tools—both physical and regulatory—that enable the distribution of information across interconnected networks.[113] Accompanying this duty is a restriction on the role that the government itself may play in directly blocking or censoring speech on these networks.[114] Such a reading of the government's *architectural* role may be unsatisfying to those legal philosophers with an unquenchable interest in determining whether any given governmental intervention in the production of speech reflects a positive or a negative vision of liberty, but perhaps as legal philosophers debate this question, the government can get on with the job that it has been doing for the last two centuries: building out spaces in which speech will thrive and networks will connect.[115]

---

111. *See* Associated Press v. United States, 326 U.S. 1, 20 (1945).

112. *See* Ammori, *supra* note 101, at 37–39 (describing the application of common carriage-style regulations that "ensured nondiscriminatory access" to a variety of communications infrastructures); *see also* Brian Stelter, *Netflix Partner Says Comcast 'Toll' Threatens Online Video Delivery*, N.Y. TIMES MEDIA DECODER BLOG (Nov. 29, 2010), http://mediadecoder.blogs.nytimes.com/2010/11/29/netflix-partner-says-comcast-toll-threatens-online-video-delivery.

113. *See* Kevin Werbach, *The Network Utility*, 60 DUKE L.J. 1761, 1779 (2011) ("The complex mesh of network-to-network interconnection is the defining characteristic of the Internet.").

114. *See* Brief of Amici Curiae Yale Law School Information Society Project Scholars et al. in Support of Neither Party at 16, FCC v. Fox, 556 U.S. 502 (2009) (No. 07-582), 2011 WL 4352230 (arguing that "the reevaluation of the constitutional basis for indecency regulations . . . offers an opportunity to clarify that the rationales for censorious broadcast regulation are irrelevant to the rationales for spectrum access regulation in general").

115. *See* Ammori, *supra* note 101, at 46–47 (enumerating governmental interventions to promote universal access to the postal service, telegraph service, telephone service, broadcast radio and television, satellite television, cable television, and the Internet).

Giving up on the governmental project of defining ideal patterns of speech and cultural interaction also represents a substantial retreat from the vision of Sunstein, Meiklejohn, Post, and others who seek to use governmental levers to promote high-value speech. The question for the remainder of this Article, then, is whether we can use a safe harbor-driven framework to promote the normative goals (that is, broadly informed democratic debate and accountable public institutions) articulated by Sunstein and Post, or whether some more aggressive intervention will be needed—either within a framework such as defamation law targeted toward protecting users from harmful information or within a framework such as copyright law targeted toward the production of information—to promote such goals. Answering this question first requires giving a more complete account of what kind of infrastructure for speech and distribution of data Congress has set up with section 512 of the DMCA and section 230 of the CDA.

III. The Novel Methods by Which Safe Harbors Promote the Growth of Speech Infrastructure

The previous Part described a fundamental historical shift in the availability of regulatory tools for the promotion of access to information. In short, when it was difficult for the average citizen to gain access to tools for speech and distribution of data, governmental officials (as well as scholars) sought to ensure that those who did have such access were tasked with the responsibility of distributing high-quality and high-value content. But with the growth of the Internet came the potential for democratization of access to services for the production and distribution of speech. Consequently, the role of the government shifted away from directly ensuring the presence of high-value information, and toward ensuring that everyone is able to speak on interconnected networks.

The following Part considers a series of conflicting rationales for how and why limitations on secondary liability evolved to enable Internet service and application providers to serve this democratizing function. Subpart A describes the technological difficulty of tasking Internet intermediaries with legal responsibility—of the kind suggested by Sunstein, the kind suggested by the Clinton white paper, and the kind suggested by the Stop Online Piracy Act—over the user-generated data that they solicit, aggregate, copy, and distribute. Subpart B examines justifications for safe harbors beyond this narrower technological or architectural rationale.

As illustrated within the following Part, the existence of these multiple, sometimes conflicting rationales results from the fact that safe harbors lack the kind of single overriding logic that characterizes more traditional interventions in information production, such as the incentive

logic of copyright law.[116] But the multiplicity of rationales for safe harbors can actually enhance their force as a method of legal intervention, as shown by the diversity of service providers and information intermediaries spawned by safe harbors. These new legal entities, in turn, represent a surprisingly diverse array of user interests, rather than a single logic of cultural production.

A. The Technological (or Architectural) Rationale for Safe Harbors

Most analyses of safe harbors and limitations on secondary liability begin with the point that the technological architecture common to many websites—an architecture premised on unmoderated user contributions, continuous edits, and shifting, unpredictable links—might not be readily adaptable to a system of full secondary liability due to the difficulties that websites and network providers face in monitoring user-generated content.[117] For instance, courts have recognized that every "month more than 30 million notices are posted to the craigslist system," and that if such postings "had to be reviewed before being put online, long delay could make the service much less useful, and if the vetting came only after the material was online the buyers and sellers might already have made their deals."[118] Google seeks to organize hundreds of billions of unique URLs and has noted that at least seventy-two hours of video are uploaded to YouTube every minute.[119] A site like Facebook or Twitter, premised on more immediate social interactions, often lacks an easy

---

116. *See supra* text accompanying notes 37–38. The logic of copyright law, described in more detail below, entails coupling exclusive rights for limited times—to incentivize the production of future works—with the eventual and permanent release of works into a public domain where they can be the basis of new creations and innovations. *See* Brief of Amici Curiae, Information Society Project at Yale Law School Professors and Fellows, in Support of the Petitioners, Golan v. Holder 132 S. Ct. 873 (2012) (No. 10-545).

117. Mark A. Lemley succinctly states the common rationale for safe harbors:

> 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.

Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. Telecomm. & High Tech. L. 101, 102 (2007) (footnote omitted).

118. Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008).

119. *It's YouTube's 7th Birthday . . . and You've Outdone Yourselves, Again*, Youtube Blog (May 20, 2012), http://youtube-global.blogspot.com/2012/05/its-youtubes-7th-birthday-and-youve.html; *see* Kent Walker, *Making Copyright Work Better Online*, Google Public Policy Blog (Dec. 2, 2010, 11:31 AM), http://googlepublicpolicy.blogspot.com/2010/12/making-copyright-work-better-online.html.

entryway for even the site's own administrators to peer deeply into social conversations taking place on the site.

The basic architecture of these sites would likely need to be reshaped in order for intermediary liability to be effectively imposed. The harm generated by a defamatory or copyright-infringing post is often instant, and given the low costs of copying and distribution on the Internet, it is difficult to ever fully rein in or delete an offending post once it exists on the Internet.[120] At the same time, the longer that a defamatory utterance—or a copyright-infringing work—is listed on one of these social sites, the more likely it is that such utterance or work will be copied and repeated by additional users, thus multiplying the site's difficulty in eliminating all copies.[121]

Any attempt to deputize a website or platform owner with a duty to eliminate such harms altogether might require the implementation of a delay, similar to the gap on live television programs, between the utterance of a post and its "broadcast" on a given site. But delay requirements would place a severe, likely insurmountable technological burden on a site premised on interactive and real-time conversations. Similarly, the elimination of safe harbors might force website administrators to spend additional time searching through and peering into their users' otherwise hidden conversations, and might consequently run afoul of users' privacy expectations and settings.[122] And to deter the rapid dissemination of multiple copies of an infringing work or defamatory statement, website administrators might need to embed rights-management code within all user-contributed content that would allow them to remotely delete copies of that content.

To be sure, these are all significant concerns. This technological (or "architectural") rationale for limiting the enforcement requirements of intermediaries cannot, however, serve as the sole justification for implementing and preserving safe harbors and other limitations on secondary liability.

First, it is somewhat incongruous to explain the creation of safe harbors primarily by reference to the technological architecture of websites that have arisen as a consequence of the operation of safe harbors. Congress certainly considered arguments relating to the

---

120. Such efforts may even be counterproductive. *See* Mario Cacciottolo, *The Streisand Effect: When Censorship Backfires*, BBC NEWS (June 15, 2012), http://www.bbc.co.uk/news/uk-18458567.

121. In addition, as the Federal Trade Commission has recognized in assessing a French proposal regarding the "right to be forgotten," First Amendment constraints may make it difficult for the government to require third parties to delete information placed on their site by users. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 70–71 n.358 (2012).

122. Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1491 (advancing, in response to net neutrality proposals, a theory of "net non-scrutiny" under which "[t]he worst thing a provider can do is scan and capture the contents of communications").

technological architecture of sites such as America Online, Yahoo!, and Prodigy while debating § 230 and § 512, but it would have been difficult for those striking compromises between rightsholders and online service providers in the late 1990s to contemplate the range of new technological architectures of sites and intermediaries that would develop over the next fifteen years.

More importantly, even acknowledging potential technological difficulties, a given access, service, search, or application provider will, in fact, frequently be in a better position than a particular user to serve as a locus for the enforcement of copyright and defamation laws.[123] Instances of copyright infringement and defamatory speech can be distributed quickly to multiple users on digitally networked platforms and yield greater harm when a larger number of users are engaged in infringement or defamation.[124] Thus the service or application provider that hosts or links to a copyrighted or defamatory work will typically be a more attractive and efficient target for an aggrieved rightsholder than an individual infringer. These providers may be able to block users—as well as instances of infringement or defamation—en masse. In addition, an offended rightsholder may find it more politically convenient and socially feasible to deputize intermediaries than to send "cops after everybody who attempts a risqué or politically sensitive search" or chase "down the origin of every offending link."[125]

Even if intermediaries face technical or legal monitoring difficulties in political contexts where such overt surveillance and policing is impermissible, they will still generally be better equipped than individual users to attempt to put the cat back into the bag. As a corollary point, a well-funded service or application provider—with comparatively deeper pockets than an infringing or defaming user—will be a more attractive target for injured parties who seek monetary recompense.

In sum, Internet intermediaries may be powerful, and their technological architectures may put severe limits on their ability to

123. *See* Brief of Amici Curiae Stuart N. Brotman et al. in Support of Plaintiffs-Appellants at 13, Viacom Int'l Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2007) (No. 10-3270), 2010 WL 5167429 ("ISPs often will be the least cost avoiders for preventing or limiting harm from copyright infringement over the Internet."); *see also* European Commission, *Application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights*, at 7, SEC (2010) 1589 final (Dec. 12, 2010) (noting "intermediaries' favourable position to contribute to the prevention and termination of online infringements" and suggesting ways to "involve them more closely" with such efforts).

124. The European Commission adopted this rationale in its analysis of whether it should limit the circumstances under which Internet providers can claim the protection of safe harbors. *See* European Commission, *supra* note 123, at 5.

125. Rebecca MacKinnon, *Commentary: Are China's Demands for Internet 'Self-Discipline' Spreading to the West?*, McClatchyDC (Jan. 18, 2010), http://www.mcclatchydc.com/2010/01/18/82469/commentary-are-chinas-demands.html (analyzing the absence of safe harbors for intermediaries in China).

monitor user actions, but with their great pervasiveness and control over a wide variety of data-delivery tools comes potential susceptibility to public or private deputization. Thus some additional rationale is needed to explain the rise of safe harbors.

B. The Co-Evolving Democratic (or Speech-Based) Rationale for Safe Harbors

A second motivation for section 512 of the DMCA and section 230 of the CDA—beyond the shaky technological rationale offered above—emerges from the fact that service, search, and application providers have facilitated a high level of user participation in scientific, cultural, artistic, and political discourse on the Internet. If the debate over safe harbors simply concerned whether intermediaries are least cost avoiders,[126] and whether intermediaries have the technological capacity to embed greater user surveillance and monitoring into their services, then it might be difficult to determine how to resolve competing claims for and against the deputization of service providers as enforcers of copyright and defamation law.[127] However, as described in the following Subpart, these safe harbors also generate a high amount of networked speech and user-contributed information, along with a legal architecture that shields this speech and information from a variety of potential threats. Accordingly, there may be a democratic interest in avoiding a distortion of the incentives of intermediaries with respect to their many dependent users,[128] and this social outcome may tilt the argument toward keeping safe harbors in place.[129]

As the following Subpart demonstrates, the jurisprudence of section 512 of the DMCA has implicitly co-evolved with the jurisprudence of section 230 of the CDA, if along a slightly different trajectory, to bring this democratic speech rationale to the forefront of any debate about the purposes of safe harbors.

---

126. *See supra* note 123.

127. *See, e.g.*, Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 Sup. Ct. Econ. Rev. 221, 226 (2006) (suggesting modifications to § 230 that would "encourage service providers to adopt the precautions that they can provide most efficiently while leaving any remaining precautions to other market actors").

128. *See* Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 Harv. J.L. & Tech. 171, 181 (2010) ("Service providers are imperfect agents for their poster-principals. These intermediaries to online speech likely have different incentives and risk sensitivities from their users, and the additional layer they represent increases information costs.").

129. *See, e.g.*, CDA, 47 U.S.C. § 230(a)(3) (2012) (finding that the "Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity"); DMCA, 17 U.S.C. § 512 (2012) (striking a balance between interests of copyright owners, intermediaries, and digital users).

1. The Dialogue Between § 512 and § 230

In analyzing the democratic justification for limitations on secondary liability, it is important first to compare how different limitations have been designed to promote different norms and different sets of democratic interests. Perhaps the most salient difference between section 512 of the DMCA and section 230 of the CDA is that the latter provision lacks a notice-and-takedown regime.[130] That is, an intermediary that relies upon the protections of section 230 of the CDA is under no obligation to remove defamatory or offensive content after being notified of its existence.

The absence of a notice-and-takedown regime in the context of the CDA, as opposed to the DMCA, can be justified on grounds that building in an obligation to remove original user *expression* upon mere notice of falsity or alleged defamation would amount to the grant of a privately enforceable "heckler's veto."[131] The broader grant of protection offered to intermediaries under § 230(c) coincides with the greater emphasis that this provision—in contrast with § 512—places upon the development of online speech.

Section 230(c) promotes speech in an indirect way: not by increasing the responsibility of parties for online speech, but instead by *limiting* the scope of who can be considered to be a "publisher or speaker" of information generated by others. Section 230(c) confines responsibility for tortious or contract-infringing speech to the speaker herself, and prevents liability for such speech from bubbling upwards to the intermediary who hosts such speech. This provision protects the distributors of speech rather than the creators of speech, but it is still, at heart, concerned with speech.[132] Section 230(c) places great emphasis on the benefits of the distribution of online speech,[133] and does not (on its face) implement any form of regulatory balancing mechanism that would allow courts to compare these benefits with the external costs that arise

---

130. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997) (rejecting notice-based liability for intermediaries).

131. *See* Reno v. ACLU, 521 U.S. 844, 880 (1997) (describing the "heckler's veto"). Analogously to the heckler's veto, the introduction of a notice-and-takedown rule to § 230(c) would enable an opponent of speech to "log on and inform" an online forum's administrator that defamatory speech was present, effectively compelling the administrator to remove that speech rather than engage in a costly and uncertain legal analysis as to whether that speech was in fact defamatory. *See* Seltzer, *supra* note 128, at 191 (noting in the context of § 512(c) that "[n]early all general-purpose providers take down content almost automatically upon receipt of a conformant notice").

132. Section 230 is not focused on the development of online media content. *See* CDA, 47 U.S.C. § 230(e)(2) (clarifying that the immunity in § 230 does not extend to the violation of intellectual property laws).

133. *See* Balkin, *supra* note 52, at 433 ("Most students . . . probably do not hear much about section 230 in their First Amendment classes, but it has been one of the most important guarantors of free expression on the Internet, at least in the United States.").

when speech harms the operation of a contract or infringes upon another person's good name or dignity.

Section 512, on the other hand, makes no reference to speech or speakers, and is instead focused on whether a service provider has knowledge of "infringement of copyright,"[134] a type of activity the suppression of which, the Supreme Court has suggested, raises more limited First Amendment concerns.[135] Unlike § 230, § 512 contains no "preamble" setting forth a litany of speech-protective goals.[136] It is again appropriate, then, that § 512(c), which is concerned with limiting the exercise of copyright entitlements—the very purpose of which are to serve as an "engine for free expression"[137]—would modulate this risk-benefit analysis in a different way, namely by building in a notice-and-takedown provision. A looser alternative rule analogous to section 230(c) of the CDA—permitting intermediaries to do nothing in the face of awareness of specific infringement—might levy too much damage upon the structural functionality of the copyright entitlement. Waiving all obligations to take down infringing materials—even in the face of express knowledge of such infringement—would, as supporters of the safe harbor point out, deprive copyright holders of "a direct, efficient, and effective remedy against infringing conduct on the massive scale made possible by participatory media platforms."[138] Put simply, deputizing intermediaries makes sense where they do in fact have the ability to control the presence of infringing content *and* where they gain some economic benefit from the presence of this content, and where deputizing an intermediary does not generate significant negative speech-related externalities. Hence the § 512 safe harbor is not so relaxed as to allow a service provider to be completely passive in the face of awareness of specific infringing content, but also not so strict as to require a service provider to monitor or affirmatively seek "facts indicating infringing activity."[139]

The takedown system in § 512(c), by setting up a line of communication between intermediary service providers and copyright

---

134. *Compare* DMCA, 17 U.S.C. § 512(c)(1)(A) (safe harbor based upon lack of knowledge of infringing material), *with* CDA, 47 U.S.C. § 230(c)(1) (safe harbor based upon declassification as "speaker or publisher").

135. *See* Eldred v. Ashcroft, 537 U.S. 186 (2003); *see also* Christina Bohannan, *Copyright Infringement and Harmless Speech*, 61 HASTINGS L.J. 1083, 1097 (2010) (noting that courts seldom apply the First Amendment in copyright infringement cases despite the fact that "copyright law burdens self-expression by restricting what people can say and write").

136. *Compare* DMCA, 17 U.S.C. § 512, *with* CDA, 47 U.S.C. § 230(a)–(b).

137. Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985).

138. Brief of Amici Curiae Intellectual Property and Internet Law Professors in Support of Defendants-Appellees and Urging Affirmance at 7, Viacom Int'l Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2007) (No. 10-3270), 2011 WL 1461438.

139. DMCA, 17 U.S.C. § 512(m) .

holders—who are better motivated than intermediaries to guard their copyrighted works and search out possible infringers—enables an efficient remedy scheme that preserves some measure of separation within this layered industry structure. In terms of an analogy to computer programming architectures, § 512(c) sets up a sort of context-specific programming interface between intermediaries and the owners of information,[140] without going so far as to allow information owners to write code that would more generally govern the behavior of information intermediaries. Section 512 implements a system where rightsholders can opt in and actively request specific takedowns, but § 512 refrains from deputizing intermediaries as *general monitoring and enforcement agents* of those rightsholders.

Together, section 512 of the DMCA and section 230(c) of the CDA risk a good deal of unregulated creativity and communication on the boundaries of copyright law and defamation law, on the theory that the rewards of such creativity—new structures and functions for online communities, as with Wikipedia,[141] YouTube,[142] Craigslist,[143] and Facebook, greater flourishing of interactive media, more robust political discourse, and 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. Section 512 and § 230 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. Congress has weighed these costs and benefits of intermediary deputization, and has concluded that the proper decision is to "provide breathing space" for platform providers and

140. *See, e.g.*, *What Is YouTube's Content ID Tool?*, YOUTUBE HELP, http://www.google.com/support/youtube/bin/answer.py?hl=en&answer=83766 (offering a system for copyright owners whose content appears on YouTube to "block, track, or monetize" that content); *see also* Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 528 (S.D.N.Y. 2010) ("In its 'Claim Your Content' system, YouTube used Audible Magic, a fingerprinting tool which removed an offending video automatically if it matched some portion of a reference video submitted by a copyright owner who had designated this service.").

141. *See generally* Ken S. Myers, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. L.J. LAW & TECH. 163 (2006) (arguing that a proper interpretation of the CDA § 230 safe harbor immunizes Wikipedia from defamation liability).

142. *See Viacom*, 718 F. Supp. 2d at 523.

143. *See, e.g.*, Chi. Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008); Dart v. Craigslist, Inc., 665 F. Supp. 2d 961, 969 (N.D. Ill. 2009) ("Section 230(c)(1) would serve little if any purpose if companies like Craigslist were found liable under state law for 'causing' or 'inducing' users to post unlawful content.").

aggregators of user-generated content "that might otherwise run afoul of copyright silos" and defamation entitlements.[144] Courts have adopted a similar understanding of these laws.[145]

2. *Using Safe Harbors to Construct and Protect Communities of Users*

One remaining question, then, is whether providing "breathing room" for intermediaries can protect *user* speech as well as intermediary aggregation of that speech. At the very least, it can be argued that the set of limitations on secondary liability in § 512 and § 230 solve a collective action problem faced by those users who are interested in participating in online communities and sharing information and perspectives with other users. This collective action problem runs roughly as follows: Users will generally be unwilling to build or participate in such communities if they are wary of litigation over defamation and copyright infringement. The first individual to share speech and information with third parties—and enable a sufficiently broad network of users to share speech and information back—would be an instant target for copyright and defamation lawsuits. A set of safe harbors that limits the responsibility of intermediaries, then, has the effect of *creating a new legal entity*—the service provider—that is separate from these original information providers, and is able to represent their collective communicative interests by virtue of this separation.

Safe harbors thus encourage intermediaries to set up platforms for communication and innovation that are maximally attractive to users by assuring such intermediaries that the *size* of the resulting community of users and the *strength* of the resulting megaphone given to users' speech will not result in correspondingly significant increases to the intermediary's potential liability for user actions. As with the shift in form from general partnerships to limited liability corporations, the presence of safe harbors enables intermediaries to cultivate and invest in a wide network of unaffiliated users without needing to engage in extensive background checks of those users. If intermediaries were liable for the activities of users, they would only "partner" with information contributors whom they vetted and trusted. But due to the presence of safe harbors, intermediaries can safely cultivate and develop information from large networks of users—just as limited liability rules enable corporations to develop large

144. Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. DAVIS L. REV. 343, 408 (2008).

145. *See* Almeida v. Amazon.com, Inc., 456 F.3d 1316, 1321 (11th Cir. 2006) ("The majority of federal circuits have interpreted the CDA to establish broad 'federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.'" (quoting Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997))).

networks of investments—without becoming personally liable for the infringing or fraudulent activities that happen to emerge upon that network. By this process, a limit on the responsibility of intermediaries for users becomes, in a strange shift, a way of encouraging intermediaries to represent the collective interests of those users in speaking and interacting with as broad a network as possible.

To make this point more clearly, it is instructive to imagine a different legal system in which Congress had never enacted § 512(c) and § 230(c). Forcing Internet access providers and website providers to internalize the legal risks associated with their users' defamatory or copyright-infringing activities would drastically alter the incentives in opening a network or platform to users and unexpected activities in the first place. Due to the large number of service and access providers through which any given action passes on the Internet, user activities would generally not be permitted until a variety of layered service providers were satisfied that the benefits of its inclusion outweighed its legal risks.[146] In order to avoid the threat of intermediary liability, Internet access providers, website providers, and even device manufacturers would need to strictly and actively police an often blurred distinction between which kinds of user activities constitute copyright infringement and defamation, and which do not.[147] Even if a given user or activity were highly unlikely to be associated with copyright infringement or defamation, a rational intermediary might nonetheless ban the user or activity just to be on the safe side of a possible penalty of up to $150,000 for each act of infringement,[148] or the penalty of a broad injunction in the case of defamation. The lack of clear definitions of copyright infringement and defamation, combined with the significant costs incurred in running afoul of such laws—particularly when violations of these laws occur in bulk—make it hard to imagine a scenario in which *any* intermediary would choose to open their service as a conduit for users and internalize the requisite risk.[149]

---

146. The list of potentially liable parties extends beyond Comcast and AT&T, and includes Internet transit providers such as Level 3 Communications and Tata Communications, web hosting providers such as Godaddy and Amazon Simple Storage Service, websites such as Facebook and Blogger, and application providers such as Zynga that use a given website's application programming interface to interact with users. Device and browser providers such as Apple and Mozilla could theoretically be held liable under a broader standard of intermediary responsibility as well.

147. Indeed, this positioning of intermediaries as copyright gatekeepers was the traditional role played by service providers up until the passage of § 512. *See* Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 685–86 (2003).

148. *See* 17 U.S.C. § 504(c)(2) (2012) ("In a case where the copyright owner sustains the burden of proving, and the court finds that infringement was committed willfully, the court in its discretion may increase the award of statutory damages to a sum of not more than $150,000.").

149. More progressive or less risk-averse service providers might develop best practices where they opted to ban "slavish" copying and uploading by users, following the rule set forth in *Bridgeman Art*

Rather than deputize intermediaries as enforcement agents of rightsholders, then, safe harbors instead portray intermediaries as *platform providers* and *aggregators of democratic discourse*. Section 512 of the DMCA and section 230 of the CDA are, under this reading, subsidies of innovation and democratic discourse, not subsidies of libel and copyright infringement.[150] Intermediaries promote user interests not by purporting to speak and take responsibility for users, but instead by acting as a fair and neutral conduit for users' speech and creative actions. These two limitations on secondary liability encourage intermediaries to adopt this role as a conduit for users by—through slightly different legal mechanisms—separating out the speech and actions of users from the speech and actions of intermediaries.

Yet while this account of § 512 and § 230 comes closer to a normative explanation of limitations on secondary liability, it still suffers from inadequate consideration of how these laws—and the networked intermediaries they generate—alter the preexisting dynamic between content providers and network providers on the Internet. Neither this account, nor the technological/architectural account given above in Part III.A, is sufficient to explain the extent to which safe harbors have restructured the development of information and communications platforms, and reshuffled the roles of public and private regulators over these platforms. The following Part seeks to explore the broader regulatory impact of § 512 and § 230 upon the national information infrastructure.

IV. Safe Harbors as a Distributed Regulatory Strategy

The previous Part argued that one result of safe harbors was the creation of a new class of service provider that, by virtue of being

---

Library, Ltd. v. Corel Corp., 36 F. Supp. 2d 191, 197 (S.D.N.Y. 1999), but permit the sharing of content that had achieved a certain degree of creative transformation. Again, however, the difficulty of making this sort of judgment—combined with the significant costs of infringement liability for making the wrong judgment—would likely result in a default assumption that *most* such user practices would be prohibited, even where the practice had a great likelihood of qualifying for the fair use defense or another exception.

150. *Cf.* David Thompson, *Fixing the CDA 230 Subsidy While Preserving Online Anonymit*y, The Volokh Conspiracy (June 10, 2010, 8:33 PM), http://volokh.com/2010/06/10/fixing-the-cda-230-subsidy-while-preserving-online-anonymity. Of course, it is arguable that neither § 512 nor § 230 strikes a perfect balance in this regard. Section 512 does not permit enough user innovation, and it provides insufficient due process protection for users whose works are subject to takedown requests from aggrieved rightsholders. *See* Seltzer, *supra* note 128, at 176. Section 230, meanwhile, permits too much user speech, and does not require intermediaries to take down obviously defaming content even when they are perfectly aware of such content and clearly capable of deleting it from their servers and blocking the users who shared it. *See, e.g.*, *AutoAdmit*, Citizen Media Law Project (Sept. 10, 2007), http://www.citmedialaw.org/threats/autoadmit#description ("According to the complaint, the two students complained about the forum postings to the AutoAdmit staff, but AutoAdmit did not remove the material. Ciolli disputes that he had any authority to remove the offensive postings.").

immunized from liability for the activities of information and content providers on its platform, gained the ability to function as an intermediary conduit for the movement and aggregation of speech and information from multiple independent sources. Part III.A portrayed this system of legislative immunities as a product of the significant technological difficulties in tasking service providers with responsibility for enforcement of copyright and defamation law on the Internet. Part III.B showed how this system of immunities eventually evolved into an intentional democratic strategy: Both the legislature and the courts used safe harbors to actively promote the development of communications and distribution platforms upon which diverse and antagonistic discourse would flow.

But the rationales for safe harbors and immunities from secondary liability are not purely technological or speech-protective in nature. This Part develops an argument that section 512 of the DMCA and section 230 of the CDA have been used as part of an emerging *regulatory* strategy to set up a layer of private intermediary watchdogs between private information owners and private infrastructure providers. With safe harbors in place, Internet intermediaries became better positioned to represent users' communicative interests than users themselves (who were not similarly immunized), and these intermediaries simultaneously emerged as key advocates for the growth of open communications infrastructure. After offering this Article's central thesis—that limitations on secondary liability function as a form of regulation—this Part situates this regulatory claim in the context of other historical tools for limiting the power of private information owners.

A. Generating a Layered Network Architecture

The basic claim made on behalf of limitations on secondary liability, up until this point of this Article, has been that even though safe harbors and immunities are geared toward Internet intermediaries, these protections ultimately inure to the benefit of users themselves. They do so by setting conditions for the development of a communications infrastructure that is more open, robust, and participatory than a similar communications infrastructure that lacks these safe harbor protections. This benefit to users takes place in spite of the fact that section 512 of the DMCA and section 230 of the CDA explicitly do not protect individual users from defamation or infringement lawsuits. If a given user were somehow to create and share millions of copyright infringing songs or videos, or issue millions of defamatory statements on her own website, that user would face massive copyright and defamation liability even if she immediately took the media and statements down from her website or off

her computer upon being notified of their illegality.[151] But where a given *intermediary* provides a platform upon which millions of users each happen to share a few copyright-infringing videos and make a few defamatory statements, that intermediary will *not* face copyright and defamation liability so long as it follows the notice-and-takedown procedures established in § 512 and does not actively shape the defaming statements.

Section 512(c) and § 230(c), then, represent a new form of regulation designed to promote the development of speech and network infrastructure without offering any explicit new protections for the users of that infrastructure. These safe harbors are not modeled on rights, which would be difficult to administer in a layered information environment with multiple stakeholders potentially laying claim to such spaces. They do not work by granting intermediaries a positive access entitlement to another party's content or identity; even if such access may still arise through the application of contractual arrangements, fair use, first sale, the public figure doctrine, or some other defense to copyright infringement or defamation, safe harbors themselves do not afford this sort of access entitlement. They do not incorporate some version of the First Amendment against the private owners of the copyrighted content or the network infrastructure that these intermediaries crawl. Nor are they modeled in accord with the single governing logic of copyright law, which trades off the embarrassment of a temporary monopoly over a creative work in order to give that work's rightsholder an opportunity to recoup investments in the work. Safe harbors do not build in time- or subject matter-based limitations into the structure of an information right that will ensure the population of a robust public domain,[152] nor do safe harbors offer statutory immunities to narrowly tailored classes of creators or users.[153]

Instead, these limitations on secondary liability enable the growth of backwater spaces for communication and technological development, and distribute responsibility for the maintenance of these spaces to a new class of intermediaries. With safe harbors in place, network providers and content owners are no longer the sole entities to determine under

---

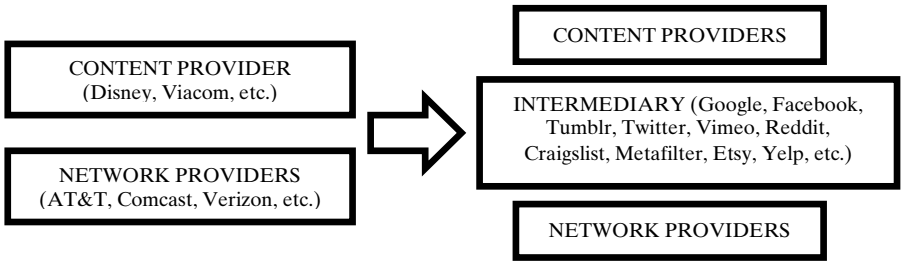
151. *See, e.g.*, Nate Anderson, *Thomas Verdict: Willful Infringement, $1.92 Million Penalty*, ARS TECHNICA (June 18, 2009, 2:32 PM), http://arstechnica.com/tech-policy/2009/06/jammie-thomas-retrial-verdict. Such an individual would not be able to claim the § 512(c) safe harbor due to her own uploading of copyrighted content. This individual could not claim the § 230(c) safe harbor, either, due to the fact that she was clearly the publisher or speaker of the original information.

152. *See infra* Part IV.C.

153. *Compare* CDA, 47 U.S.C. § 230 (2012) (offering immunity to any "provider or user of an interactive computer service"), *and* DMCA, 17 U.S.C § 512 (2012) (offering conditional immunity to "service providers"), *with* 17 U.S.C. §§ 107–20 (identifying classes of users such as librarians and educators that will receive immunity from the enforcement of copyright law in specific contexts of use).

what conditions user access, participation, and innovation shall take place within these spaces.

Instead, these limitations on secondary liability enable the growth of backwater spaces for communication and technological development, and distribute responsibility for the maintenance of these spaces to a new class of intermediaries. With safe harbors in place, network providers and content owners are no longer the sole entities to determine under what conditions user access, participation, and innovation shall take place within these spaces—a distribution that is designed to avoid the dangers of data enclosure and regulatory capture while still retaining the practical effect of enlarging user access and promoting diverse and antagonistic speech.[154]



By ensuring that platform providers are not legally responsible for the speech of users, the § 230(c) immunity frees providers to solicit a more diverse range of speech on their platforms.[155] Similarly, by ensuring that search companies, network providers, and solicitors of user-generated content need not act as the copyright enforcement arms of media companies, the § 512 safe harbor frees providers to solicit and aggregate a much broader range of creative resources on their platforms than would otherwise be possible.[156]

This distribution of responsibility gives rise to a number of positive spillover effects. First, safe harbors enable the population of a ready domain of creative resources. Wide access to common pool resources increases participation in scientific and cultural meaning-making and also increases the likelihood that the products of such participation will have

154. The line between regulation and deregulation, of course, is not always clear. Many have described section 230(c) of the CDA and section 512(c) of the DMCA as deregulatory moves designed to inhibit the government from interfering with the growth of private information providers and carriers on the Internet. *See* Adam Thierer, *The Case for Internet Optimism, Part 2: Saving the Net from Its Supporters*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 139 (Berin Szoka & Adam Marcus eds., 2010). Some have celebrated these laws, calling section 230 of the CDA the "Communications Democracy Act," *see* Jerry Berman, while others have argued that these laws pose significant threats to the capacity of individuals and copyright holders to be safe from defamatory or infringing activities on the Internet. *See infra* Part V.B.

155. *See supra* Part I.B.

156. *See supra* Part I.A.

widespread democratic legitimacy.[157] Users will contribute existing and new information goods—and will have the opportunity to use these goods—on platforms that have taken advantage of safe harbor protections. Simply put, it is likely that more information will be available from a wider range of sources and accessible to a wider range of people as a result of the operation of safe harbors.

Second, beyond increasing access to information, these services generate new infrastructures on which new forms of action become possible. The implicit purpose of creating this breathing space around the edges of the law is to encourage the development of a wide range of potential business models and organizational tools on the *edges* of a given network—models and tools that would generally not have been developed by information owners or infrastructure providers themselves. If these legislative, judicial, and regulatory standards were not in place, it is likely that the development of user speech and intermediary infrastructures would be contingent upon the ability of aggregation and distribution networks to enter into vertical licensing arrangements with (a) the owners of the telecommunications networks on which they transmit information and (b) the owners of the content they crawl and organize.[158] Safe harbors from copyright liability and immunities from defamation liability, along with regulatory separations of telecommunications services from information services, enable intermediaries on the Internet to act without needing to be linked in to traditional content providers (on the one hand) and traditional programming distributors and Internet access providers (on the other hand).

Third, this delinking of intermediary aggregation and distribution networks from the control of "last mile" network owners, in turn, tends to increase the options and lower the barriers to entry for independent developers and content providers who want to reach a broad audience without becoming dependent upon incumbent distribution networks. For instance, rather than needing to build server farms or content-delivery networks or even more prosaic features such as mapping or document-creation software and crowdsourcing tools, a new data or application

157. *See* Elizabeth Anderson, *The Epistemology of Democracy*, 3 EPISTEME 8, 14 (2006), *available at* http://muse.jhu.edu/journals/episteme/v003/3.1anderson.html (describing ways in which democracy functions by "pooling . . . asymmetrically distributed information for decision-making" and engaging diverse participants to discuss problems of public interest, thus both "mak[ing] maximal use of . . . situated knowledge" and granting democratic legitimacy to actions taken subsequent to such discussions).

158. Although YouTube is now turning a profit and thus capable of licensing content from third-party providers, especially with funding support from its owner Google, when it first emerged as an independent video intermediary, it had no such capabilities, and likely would not have been able to survive as a user-generated platform if information owners such as Viacom and NBC had been able to secure licensing fees whenever a user uploaded their content. *See* Brief for Defendants-Appellees at 76, Viacom Int'l Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2007) (No. 10-3270), 2011 WL 1356930.

provider can simply tap into the interface that a service provider such as Google and Amazon provides. By using a service such as Dropbox, a wide variety of website and application developers can obtain access to storage and information-sharing tools without expending resources on server and network administration. By using Amazon's remote computing services, it becomes simple to set up externally hosted servers, databases, and account management tools. The result is a reduction in entry barriers (which often comes in exchange for granting those new infrastructure owners some additional degree of centralized control and oversight over third-party use of their infrastructures).

Fourth, the distribution of responsibility from the center of a network to its edges enables the development of a wider set of rules and norms to govern these distributed activities. Such secondary tools may be both legal and technological in nature. Secondary legal tools may come from above, for instance, in the form of private terms of service agreements determined by platform providers. In some cases, platform providers may enter into collaborative arrangements with users to determine the structure of these rules.[159] Other secondary tools may come from outside a given firm, for instance, in the case of platform-agnostic arrangements such as the Creative Commons ShareAlike license and the General Public License[160]—licensing mechanisms that set up a protected space in which those who create, modify, and distribute creative works voluntarily agree to share back those creations and modifications with any other entities that agree to adhere to the same principles.[161] Or norms may emerge

159. *See, e.g.*, Sharon Gaudin, *Facebook Gives Users a Set of Rights and a Vote on Policy*, COMPUTERWORLD (Feb. 26, 2009, 12:00 PM), http://www.computerworld.com/s/article/9128696/Facebook_gives_users_a_set_of_rights_and_a_vote_on_policy; Mark Zuckerberg, *Voting Begins on Governing the Facebook Site*, THE FACEBOOK BLOG (Apr. 16, 2009, 12:48 PM), http://blog.facebook.com/blog.php?post=76815337130. *But see* Elliot Schrage, *Proposed Updates to Our Governing Documents*, THE FACEBOOK BLOG (Nov. 21, 2012, 9:40 AM), http://www.facebook.com/notes/facebook-site-governance/proposed-updates-to-our-governing-documents/10152304935685301 (describing Facebook's proposal to end the process of soliciting user votes on its site governance policies "in favor of a system that leads to more meaningful feedback").

160. *See, e.g.*, *Creative Commons Attribution-ShareAlike License 3.0*, CREATIVE COMMONS, http://creativecommons.org/licenses/by-sa/3.0/us (last visited Dec. 7, 2012); *GNU General Public License Version 3*, GNU (June 29, 2007), http://www.gnu.org/licenses/gpl.html.

161. These tools are not premised on the public domain, or on some preordained dividing line "between the realm of property and the realm of the free." *See* James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33, 66 (2003). Rather, they rest on licenses which themselves rest on the exercise of intellectual property rights. A grant of such a license is often conditioned upon the licensee's compliance with terms such as the duty to distribute modifications to the licensed work under the same terms as the initial license. *See, e.g.*, *Creative Commons Attribution-ShareAlike License 3.0*, *supra* note 160 ("If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one."); *GNU General Public License Version 3*, *supra* note 160 ("[I]f you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code."). As James Boyle

from single platforms: By enabling users to edit text on a common platform and observe, discuss, manage, and defend the edits of others, the collaboratively edited Wikipedia has become an essential resource for those seeking to learn more about a given topic *and* to offer better descriptions of that topic, and norms associated with this editing process have spread outside the context of Wikipedia entries.[162] Finally, this distribution of responsibility may give rise to a need for more systematic legal tools to solve problems such as the "ownership thicket" that crops up when too many interlocking rights stand in the way of downstream innovation,[163] the toll-keeping problem that arises when too many intermediaries interact with data as it passes from one user to another, as well as attempts by network and platform owners to leverage their control over layers of infrastructure in order to limit competition or the flow of data at other layers.[164]

Finally, the creation of the "intermediary layer" helps to solve a problem in the political economy of telecommunications lawmaking and regulation.[165] By enabling the addition of countless new websites focused on the solicitation of user-generated content and new distributors untethered to physical network owners, § 230, § 512, and the principle of network neutrality yield a new layer of online service providers between media providers and telecommunications providers. If it were not for this intermediary layer, it would be hard to imagine Congress and the FCC having the same conversations about issues such as network neutrality; instead, the likely topic of debate would be how to regulate carriage contracts between network providers and content providers—a conversation that would look more like the decades-old debate around "must carry" regulations.[166] But this carriage problem is partially solved by the development of distributed intermediaries that challenge the

---

has observed, these licenses are part of an attempt "to build a living ecology of open code, where the price for admission was your commitment to make your own incremental innovation part of the ecology." Boyle, *supra*, at 65.

162. *See generally* JOSEPH REAGLE, GOOD FAITH COLLABORATION: THE CULTURE OF WIKIPEDIA (2010).

163. *See generally* MICHAEL HELLER, THE GRIDLOCK ECONOMY: HOW TOO MUCH OWNERSHIP WRECKS MARKETS, STOPS INNOVATION, AND COSTS LIVES (2008) (describing how a "tragedy of the anticommons" resulting from a multiplicity or fragmentation of rightsholders can forestall downstream coordination by those who seek to engage in beneficial uses of the property or information protected by such rightsholders).

164. *See, e.g.*, United States v. Microsoft Corp., 253 F.3d 34 (D.C. Cir. 2001); United States v. AT&T, 552 F. Supp. 131 (D.D.C. 1982).

165. *See* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 631–32 (1994) (describing legal requirements imposed upon cable systems to carry varying numbers of broadcast television stations based upon the size of the cable system).

166. The Open Internet Report and Order developed by the FCC to oversee the activities of Internet access providers has, of course, still been subject to jurisdictional, administrative, and constitutional challenge. *See* Notice of Appeal, Verizon v. FCC, No. 11-1355 (D.C. Cir. Sept. 30, 2011) (No. 11-1355); *see also* Petition for Review, Free Press v. FCC (1st Cir. 2011) (No. 11-02123).

power of rightsholders and network providers, both in an economic sense and in the context of regulatory proceedings. Instead of needing to set up a complex regulatory framework—which might be subject to capture by information and network owners—the remaining challenge for the government is to exercise sufficient oversight to preserve the stability of the ecosystem's different layers.[167]

In summary, then, safe harbors, limitations on intermediary liability, and network nondiscrimination standards have presented a way for Congress and regulatory agencies to devolve control away from traditionally powerful rightsholders and network providers, and toward a new class of online service providers and information intermediaries. The growth of these intermediaries has largely taken place outside the public legal framework of copyright and defamation laws—as well as outside the control of network infrastructure providers. And the result has been, on balance, the creation of a broader range of competitive distribution and interaction platforms.

B. Promoting Diverse Legal Architectures

The impact of § 512, § 230, *Sony v. Universal*, and network nondiscrimination standards becomes even more apparent when the regulatory "logic" of safe harbors is compared with the logic of more traditional interventions in information law and policy. In comparison to intellectual property and defamation laws, safe harbors shift the locus of control for soliciting, organizing, and distributing information away from single, centralized entities.

Consider three sets of laws relevant to the development of speech on the Internet: defamation law, copyright law, and "safe harbor" law. All of these laws are, at least in theory, necessary conditions for a functioning Internet. Safe harbors—such as section 512(c) of the DMCA and section 230(c) of the CDA—minimize the legal exposure faced by developers of the information superhighway's infrastructure, justifying investment in the conduits and communications platforms that provide the Internet's raw connectivity. Intellectual property laws ensure that this superhighway attracts a large number of roadside attractions—copyright

167. The Internet's different layers hang together through a combination of rules designed to promote the unconstrained cultivation and development of content by intermediaries (including websites, search engines, application providers, and other information platforms) and other rules designed to ensure that providers of the physical and networked infrastructure of the Internet do not regularly exercise any market power to inhibit competition among those higher-layer content and application providers. These seemingly contradictory policies—imposing regulation upon Internet access and connectivity providers while simultaneously immunizing from liability the content and application providers that users reach through access providers—contribute to the preservation of the layered architecture of the Internet.

law, in particular, encourages content and information producers to create and share works that might not otherwise be distributed in the absence of rights protections.[168] Finally, at the level of the individual user, privacy and defamation laws protect "the individual's right to the protection of his own good name,"[169] thus assuring the integrity of individual users' identities and promoting widespread adoption and use of the Internet.

But while the *purposes* of these laws may seem roughly compatible, these laws operate in different, often conflicting ways, and embody different forms of regulation. Copyright, defamation, and privacy laws, on one hand, operate by setting up individual entitlements and exclusive rights. Upon violation of such rights, these laws offer some measure of compensation, whether the harm takes the form of defamatory falsehood or unlicensed use of a protected expression or invention.[170] This is one form of a regulatory strategy, and it requires the government to design property-like entitlements and to adjudge where limited exceptions to those entitlements are justified.[171]

Safe harbors and immunities from secondary liability, on the other hand, do not work by granting and enforcing a temporary monopoly over a given expression in order to encourage its creation, nor do they grant individuals an analogous right over control of the integrity of their identity. Rather than setting up new exclusive rights or individual entitlements, safe harbors promote the leakiness of these rights and entitlements in networked spaces, rendering them less enforceable. This is another form of a regulatory strategy, albeit one not based on vesting control over the organization and distribution of information in the hands of a single entity.

---

168. *See* S. REP. No. 105-190, at 8 (1998) ("Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy."). *See generally* PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY: FROM GUTENBERG TO THE CELESTIAL JUKEBOX (2d ed. 2004).

169. Gertz v. Robert Welch, Inc., 418 U.S. 323, 341 (1974).

170. *See, e.g.*, *id*. (describing "compensation of individuals for the harm inflicted on them by defamatory falsehood" as the state interest underlying libel law).

171. The traditional economic justification for copyright law takes the following rough shape: Social welfare is optimized where "resource production and consumption are . . . characterized primarily by entitlements to individual resource units, held individually and allocated via market mechanisms." Madison et al., *supra* note 62, at 664. If such entitlements to individual resource units do not already exist (or cannot be enforced), the government, in order to promote individual stewardship and optimize social welfare, must intervene to create and enforce such property-like entitlements. *See* Tim Wu, *Copyright's Communications Policy*, 103 MICH. L. REV. 278, 329 (2004). During the length of the copyright or patent term, such author or inventor will extract licensing fees from others who would like to use or access her work, thus enabling her to recoup the various costs incurred in the production and distribution of her work. Aggregated over a wide variety of creative actors, this Demsetzian model is intended to produce dynamic innovative efficiency on a scale sufficient to overcome the static inefficiencies associated with placing a non-zero price on the copying and distribution of otherwise nonrivalrous and nonexcludable digital goods.

What safe harbors supply in the place of the general and uniform logic of intellectual property rights is a *patchwork* of rules to govern the development and aggregation of speech and action in online contexts. In contrast to copyright law, safe harbors generate a *variety* of legal infrastructures capable of accounting for (and further encouraging) a diversity of motivational patterns in different online contexts. Safe harbors rest on the implicit premise that a single rational economic model of motivation and distribution will not be equally applicable in all scientific, artistic, and communicative contexts.[172] Instead, safe harbors enable Internet intermediaries and application developers to design a variety of low-transaction-cost communities around different models for sharing both traditionally licensed and user-generated material, the norms of which will vary based on individual decisions made by their operators and users.

For these reasons, efforts to implement a *generalized* safe harbor rule—one that would replace the current patchwork of such rules and apply to all contexts of online information use and distribution—will likely be unsuccessful.[173] The fundamental diversity of safe harbors—diversity in terms of the rationales underlying safe harbors, the functional characteristics of safe harbors, and the legal infrastructures generated by safe harbors—stands in the way of such attempts to consolidate safe harbors under a single umbrella. The decentralized beneficiaries of safe harbors may be able to work together to promote common interests in maintaining that decentralization, but will be hard-pressed to identify a common logical account of how safe harbors work.

C. Situating Safe Harbors Within Historical Tools for Limiting the Power of Private Information Owners

Finally, to understand the broader regulatory impact of safe harbors, it is useful to think about what the Internet might look like if no third party intermediaries or service providers were permitted to stand between Internet users and information owners. James Grimmelmann, in a chapter criticizing the concept of search neutrality, offers up a vision of "the Hobbesian world of the unmediated Internet, in which the richest

172. One lesson of safe harbors, construed broadly, is that we do not need a doctrinal conception of a "universal order" to understand and promote human creativity; rather, "experiments in cooperation" can more effectively move us down this road. *See* Richard Rorty, *The Priority of Democracy to Philosophy*, *in* The Virginia Statute for Religious Freedom 257, 274 (Merrill D. Peterson & Robert C. Vaughan eds., 1988).

173. Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. on 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).

voices are the loudest, and the greatest authority on any subject is the spammer with the fastest server."[174] Some argue that we already lack efficient external sorting mechanisms and filters with respect to the wide variety of available content and voices on the Internet, while others contend that the filters we do have are increasingly dominating our political and cultural lives.[175] Sunstein hypothesizes a "world of perfect filtering" in which "tens of millions of people are mainly listening to louder echoes of their own voices."[176] Frank Pasquale and others, in articles calling for regulatory oversight of search providers, have argued that intermediaries themselves now exercise unregulated control over the organization of information,[177] in spite of neutral-sounding promises by Google and others to "organize the world's information and make it universally accessible and useful."[178]

These two critiques offer competing characterizations of the locus of control over information. Pasquale's concern is that control over the *organization* of information will devolve—through a combination of secrecy, proprietary claims over sorting algorithms and essential organizational tools, and simple network effects—into more general control over the infrastructures on which information flows, thus rendering it difficult to challenge existing organizational models or develop meaningful alternative models. Grimmelmann's response is that interventions to neutralize the organizational tools of intermediaries—interventions of the type that Pasquale suggests—will enable those who own websites and those who own servers to exercise unchecked control over presentation of information and interaction with users, thus making it harder for intermediaries to organize all of that information (and all of those interactions) in a way that works to the benefit of users. In short,

---

174. James Grimmelmann, *Some Skepticism About Search Neutrality*, *in* THE NEXT DIGITAL DECADE, *supra* note 154, at 435, 459. Grimmelmann concludes that the "web is a place where site owners compete fiercely, sometimes viciously, for viewers and users turn to intermediaries to defend them from the sometimes-abusive tactics of information providers." *Id*.

175. *See, e.g.*, JAMES R. BENIGER, THE CONTROL REVOLUTION: TECHNOLOGICAL AND ECONOMIC ORIGINS OF THE INFORMATION SOCIETY (1986); ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU (2011); CASS R. SUNSTEIN, REPUBLIC.COM 2.0 (2007) (contrasting the thesis of the "daily me" with the "daily we").

176. SUNSTEIN, *supra* note 175, at 13, 43–44.

177. *See, e.g.*, DAWN C. NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE (2009); Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149, 1185 (2008) ("Search engines . . . often function not as mere satisfiers of predetermined preferences, but as shapers of preferences.").

178. *Google Corporate Information*, GOOGLE, http://www.google.com/about/company (last visited Dec. 7, 2012). Noting the strong organizational claims made by search providers, Pasquale argues that "[t]here are many parallels between dominant search engines and dominant carriers: at each layer intermediaries accumulate great power over the structure of online life." Frank Pasquale, *Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines*, 2008 U. CHI. LEGAL. F. 263, 298.

Pasquale worries that intermediaries, as "essential cultural and political facilit[ies]" in themselves,[179] have too much power to shape and manipulate information, whereas Grimmelmann worries that the entities *intermediated* by search and application providers—rightsholders on one end, and owners of server infrastructure on the other end—will be granted too much power to shape and manipulate information and to confuse and manipulate users, as a result of Pasquale's suggested disintermediation.

In evaluating these competing claims, and in considering how limitations on secondary liability can help both to solve and to complicate the problem of control over information, it is useful to examine historical attempts to limit the aggregation of control over the flow of information. Courts, Congress, and regulatory agencies have all, over the years, developed tools to combat—and sometimes to enable—this aggregation of control.

The oldest tool for ensuring that private information owners do not exercise control over information flow in a way that inhibits public discourse is an artifact or contour of copyright law (or, some would say, an intangible commons that predates the introduction of copyright): the public domain.[180] Additional Congressional tinkering with the scope and duration of copyright took place within specific, narrow contexts of information use.[181] Courts and regulators, meanwhile, began to articulate a potential public right of access to certain forms of broadcast media, in order to combat what even skeptical courts recognized as the increasing concentration of media ownership and the tendency to "place in a few hands the power to inform the American people and shape public opinion."[182]

All these projects, to some extent, failed, for a variety of administrative, constitutional, and political reasons.[183] In part, these failures had to do with a reluctance to account for the dangers that arise when the government seeks to design a regulatory framework to balance public against private interests within a complex industry. In the case of attempting to broaden copyright statutes to account for different contexts

179. Frank Pasquale, *Dominant Search Engines: An Essential Cultural & Political Facility*, *in* THE NEXT DIGITAL DECADE, *supra* note 154, at 401, 402.

180. *Second Enclosure Movement*, *supra* note 161, at 39; *see* Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965, 1023 (1990) ("The public domain . . . . reserv[es] the raw material of authorship to the commons, thus leaving that raw material available for other authors to use.").

181. *See* 17 U.S.C. §§ 108–21 (2006).

182. *See, e.g.*, Miami Herald Publ'g Co. v. Tornillo, 418 U.S. 241, 250 (1974); Red Lion Broad. Co. v. FCC, 395 U.S. 367, 390 (1969) ("It is the purpose of the First Amendment to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail, rather than to countenance monopolization of that market, whether it be by the Government itself or a private licensee."); *see also* Barron, *supra* note 82, at 1666–70.

183. *See supra* Part II.

of information use, problems arose as Congress was forced to account both for the range of potential contexts of uses of copyrighted materials and the diversity of potential stakeholders affected by such contextual uses.[184] The copyright statutes that emerged from protracted negotiations between these stakeholders became lengthier and more unmanageable[185] as Congress sought to bend the statutes to solve each emerging conflict.[186] Well-organized private interests tended to prevail—as against a poorly organized set of public interests[187]—in arguing for extensions of copyright protection, sometimes even into areas where no such protection had existed in the past.[188] Even interventions designed to support the public interest, such as the introduction of termination rights, mired artists in litigation with copyright owners[189] and prompted uncertainty over the long-term stability of Creative Commons licenses and the General Public License.[190] And initial judicial articulations of limits on the scope and duration of exclusive rights[191] proved to be less than durable.[192]

These projects began to fail on constitutional grounds as well. Yochai Benkler notes that "First Amendment claims have more commonly been used to retard, not foster, efforts aimed at enhancing the availability of information from 'diverse and antagonistic sources' and the capacity of individuals effectively to express themselves."[193] For instance, courts used the First Amendment to strike down provisions including the FCC's video dial tone regulations, which would have required telephone companies to

---

184. *See* Litman, *supra* note 26, at 3 ("Copyright-intensive businesses have come to Congress insisting on new specifications to solve new problems. In the ensuing process of inter-industry negotiations to tailor statutory proposals to the quirks and caprice of affected interests, the specifications have attracted a swarm of limitations, qualifications, restrictions, and conditions as a compliant Congress inserted them into the law.").

185. Compare the length of the Statute of Anne, 8 Ann. c. 21 (1710), to the Copyright Act of 1790, ch. 15, 1 Stat. 124 (1790), to the Copyright Act of 1909, ch. 320, 35 Stat. 1075-88 (1909), to the size of the Copyright Act today (over 200 pages), 17 U.S.C. §§ 101–1332 (2006).

186. *See* Litman, *supra* note 26, at 3–5.

187. *See* Boyle, *supra* note 161, at 72 ("[P]ublic decisions are particularly likely to be bad when concentrated and well-organized groups with stable, substantial, and well-identified interests face off against diffuse groups with high information costs whose interests, while enormous in the aggregate, are individually small.").

188. *See* Uruguay Round Agreements Act, 17 U.S.C. § 104A; *see also* Brief of Amici Curiae, Information Society Project at Yale Law School Professors and Fellows, in Support of the Petitioners, *supra* note 116.

189. *See* Larry Rohter, *Record Industry Braces for Artists' Battles over Song Rights*, N.Y. TIMES, Aug. 16, 2011, at C.1.

190. *See* Timothy K. Armstrong, *Shrinking the Commons: Termination of Copyright Licenses and Transfers for the Benefit of the Public*, 47 HARV. J. ON LEGIS. 359 (2010).

191. *See* Graham v. John Deere Co. of Kan. City, 383 U.S. 1, 6 (1966).

192. *See* Eldred v. Ashcroft, 537 U.S. 186, 221 (2003); *see also* Golan v. Holder, 132 S. Ct. 873 (2012).

193. YOCHAI BENKLER, PROPERTY, COMMONS, AND THE FIRST AMENDMENT: TOWARDS A CORE COMMON INFRASTRUCTURE 34 (2001).

offer video programming on a common carriage model.[194] This result, coupled with the increasing shakiness of the *Red Lion*[195] justification for limited constitutional scrutiny of spectrum regulations,[196] heralded an era in which formerly regulated entities increasingly sought to challenge both direct and indirect governmental regulation of information environments.[197]

Finally, many of these policy frameworks inadvertently reified the position of the parties they sought to regulate.[198] Enhancements to the scope, duration, and enforceability of exclusive rights under copyright law, for instance, have enabled original publishers and owners of information to exercise greater degrees of control over downstream uses of that information.[199] Beyond opening the door to regulatory capture, such frameworks have often been insufficiently flexible to account for new and unanticipated actions within a given industry.

Safe harbors seem to offer the promise of a simpler regulatory solution. They suggest that we can slowly transition away from the project of creating ideal patterns of content and culture and instead open the door not just toward diverse and antagonistic *speakers*, but also toward diverse and competitive regulatory frameworks.

The question, then, is whether in comparison to the interventions listed above, a safe harbor-driven regulatory strategy will more effectively protect democratic discourse, promote user participation, limit information and infrastructure owners' control over data flow, and limit regulatory capture. The final Part of this Article attempts to answer this question.

---

194. *Id.*; *see* Chesapeake & Potomac Tel. Co. of Va. v. United States, 42 F.3d 181 (4th Cir. 1994), *vacated and remanded for consideration of mootness*, 516 U.S. 415 (1996).

195. Red Lion Broad. Co., Inc. v. FCC, 395 U.S. 367 (1969) (justifying limited First Amendment scrutiny of spectrum regulations based upon historically and technologically contingent circumstances such as the "scarcity of broadcast frequencies").

196. *See* Brief of Amici Curiae Yale Law School Information Society Project et al. in Support of Neither Party, *supra* note 114, at 6–7 (describing a basis for limited First Amendment scrutiny of regulations of broadcast spectrum).

197. *See, e.g.*, Notice of Appeal, Verizon v. FCC, No. 11-1355 (D.C. Cir., Sept. 30, 2011) (challenging the FCC's Open Internet Order on jurisdictional and constitutional grounds); Notice of Appeal, Cellco Partnership d/b/a Verizon Wireless v. FCC, No. 11-1135 (D.C. Cir. May 13, 2011) (challenging an FCC order requiring facilities-based providers of commercial mobile data services to offer data roaming arrangements to other such providers on commercially reasonable terms).

198. *See, e.g.*, STEVE COLL, THE DEAL OF THE CENTURY (1986) (describing the history of AT&T from the 1919 Kingsbury Commitment until Judge Greene's oversight over the breakup of the company in 1982); *see also* TIM WU, THE MASTER SWITCH (2010) (describing historical instances of regulatory capture at the Federal Communications Commission).

199. *See* Nicholas Bramble, Ex Parte Submission, In the Matter of a National Broadband Plan for Our Future, GN 09-51 (Dec. 15, 2009), *available at* http://apps.fcc.gov/ecfs/document/view?id=7020353210 (describing numerous ways in which educational uses of content have been barred as a result of the lack of notice and registration requirements in copyright law and the difficulty of litigating questions around the fair use defense).

V. The Path of the Cyberlaw

One consequence of the "incompleteness" of the safe harbor project, as described above, is that while § 512, § 230, and other limitations on secondary liability have given rise to a wealth of new functionalities and services on communications networks, they have *not* resulted in a single public domain that is common and free for all to use.[200] Instead, safe harbors have distributed the basic functionality of a public domain over a wide variety of private information and communications providers, resulting in the radical decentralization of the public domain and the growth of a series of overlapping "private domains."[201] This devolution of responsibility for information network management from Congress and governmental regulators to networked intermediaries represents a serious shift in governmental priorities: away from directly ensuring the presence of high-value information, and toward setting conditions for the development of communications infrastructure in which such information is likely to blossom.

The question for the remainder of this Article, then, is not whether this distribution of responsibility has taken place; it is whether a devolution of the sort we have witnessed with the rise of safe harbors can be a useful and sustainable model for future interventions in Internet and information policy, or whether some more aggressive set of interventions and regulations will be necessary. In posing this question, this final Part seeks to understand what a regulatory strategy driven by safe harbors does to our understanding of the public or private character of the Internet.

The first Subpart below examines the consequences of the fact that the strength of the Internet as a source for diverse and antagonistic sources of information is now contingent upon the cooperation of various private providers implementing private contractual agreements. When public protections are outsourced to private service providers in this manner, who remains to take democratic responsibility for management of the Internet's ecosystem and development of "an infrastructure of free expression"?[202] The second Subpart suggests a number of ways in which a retreat from the incentive model of information policy interventions opens the door to new forms of public investment in infrastructure and

---

200. *See supra* Part III.

201. *See* Paul Starr, *The Electronic Commons*, The American Prospect, Mar. 27–Apr. 10, 2000, http://www.princeton.edu/~starr/articles/articles00/Starr-ElectronicCommons-3-00.htm ("[T]he Internet provides incentives for commercial producers of intellectual property to shift from exclusive, high-priced forms of distribution to more open, low-priced, or free distribution—in short, from proprietary channels of communication to what I'll call the 'commercial public domain.'").

202. *See* Balkin, *supra* note 54, at 432 ("A system of free speech depends not only on the mere absence of state censorship, but also on an infrastructure of free expression."); *see also* Ammori, *supra* note 101, at 68–72.

network interconnection points, and describes tools that legislators and regulators can use to reintegrate broader legal standards into this legal backwater.

A. Tradeoffs Implicit in Private Ownership of Infrastructure for Speech and Innovation

Because the Internet is composed of multiple layers and is governed by a diverse range of public and private legal regimes, those who argue for a fully regulatory or fully deregulatory approach to the Internet will only be telling part of the story. Private providers may sometimes erect pervasive and coordinated constraints and regulations upon users, while public regulators may sometimes stand as bulwarks against these privately imposed limitations on Internet use.

1. Insufficient Protection of Information Intermediaries

The safe harbor regulatory strategy articulated in this Article involves the development of a separate layer of intermediaries between content owners and infrastructure owners. Such intermediaries, this Article suggests, may be able to mediate the concerns of such owners and protect users against the possibility that rightsholders or access providers will leverage their control to inhibit user freedom or charge supracompetitive access rates.

But a system of regulation based solely on implementing safe harbors may be insufficient to protect intermediaries from those entities that control neighboring layers of the Internet's infrastructure. Intermediaries require an environment where multiple modular networks are interconnected,[203] and can be scanned, searched, and systematized at will.[204] In the past, this interconnectivity was generated in large part by Internet access providers themselves—higher-layer information services drove users to demand connectivity services in larger numbers and at increasingly faster speeds, to the benefit of the access providers selling those connectivity services.[205] However, the market-driven consensus

203. *See* Boyle, *supra* note 161, at 46 ("For the whole structure to work without large-scale centralized coordination, the creation process has to be modular, with units of different sizes and complexities, each requiring slightly different expertise, all of which can be added together to make a grand whole.").

204. *See* Kevin Werbach, *Only Connect*, 22 Berkeley Tech. L.J. 1233, 1250 (2008) ("Though widely described as one network, the internet is actually a collection of several thousand independent networks, whose common characteristic is an agreement to interconnect to deliver internet protocol (IP) datagrams.").

205. *See* Joseph Farrell & Philip J. Weiser, *Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age*, 17 Harv. J.L. & Tech. 85, 89 (2003) (describing how increases in the value of upstream information services lead to corresponding increases in demand for the access services through which users reach such information

among Internet access providers regarding the provision of stable and commodified connectivity services may be in jeopardy.[206]

As the market for Internet access reaches saturation, at least among high-income users, the flat rates that Internet access providers charge to users may increasingly become an insufficiently flexible mechanism for access providers to increase profits from year to year. The result may be either a shift away from flat-rate pricing, or a shift away from the provision of stable, commoditized, relatively undifferentiated Internet access services by different providers and toward a more specific set of agreements and limitations placed by different Internet access providers upon their users. This latter shift could balkanize the open Internet into a series of carrier-specific Internets and preclude the development of "universal" intermediaries that can be accessed by any Internet user and that themselves can solicit and organize the content of any Internet information provider.

Hence, given the possibility of the market failure of the provision of interconnected modular networks and weakening of the concept of the Internet as a common substrate to which anyone is welcome to connect and build upon,[207] it may be necessary to search for new private or public mechanisms to promote this kind of interconnection.[208] To some extent, policymakers need not reinvent the wheel when engaging in such a search for tools to promote modular technical architectures. With *Carterfone*, the *Computer II* decision, and the recent *Open Internet Report and Order*, the FCC has sought to maximize the modularity[209] and interconnectivity of telecommunications networks.[210] The result of this

---

services).

206. *See* Preserving Open Internet, Broadband Industry Practices, 74 Fed. Reg. 62,638, 62,640 (proposed Nov. 30, 2009) (to be codified at 47 C.F.R. pt. 8) (noting that access providers may gain both the ability and the incentive to place restrictions and paywalls on the information and applications accessed by users); *see also* Werbach, *supra* note 113, at 1779–84 (describing an interconnection dispute between Comcast and Level 3).

207. *See* Susan P. Crawford, *The Internet and the Project of Communications Law*, 55 UCLA L. REV. 359, 389 (2007) ("[T]he Internet . . . can also provide a substrate that enables new ideas and new forms of social organisms to emerge, created by many different decisions to pay attention.").

208. *See* Werbach, *supra* note 204, at 1294–97.

209. Modular architectures enable participants at various layers of a network to work on subparts of that network without needing to coordinate their work with participants at other layers. *See* ZITTRAIN, *supra* note 36, at 130 (2008) ("[T]he Internet exists in layers—physical, protocol, application, content, social. Thanks to the modularity of the Internet's design, network and software developers can become experts in one layer without having to know much about the others.").

210. Amendment of Section 64.702 of the Commission's Rules and Regulations, Final Decision, 77 F.C.C. 2d 384, 420 ¶ 96 (1980) (Computer II Final Decision), *modified on recon.*, 84 F.C.C. 2d 50 (1980) (Computer II Reconsideration Order), *modified on further recon.*, 88 F.C.C 2d 512 (1981) (Computer II Further Reconsideration Order), *aff'd sub nom.*, Computer & Commc'ns Industry Ass'n v. F.C.C., 693 F.2d 198 (D.C. Cir. 1982), *cert. denied*, 461 U.S. 938 (1983), *aff'd on second further recon.*, F.C.C. 84-190 (1984); Preserving the Open Internet, 76 Fed. Reg. 59,192, 59,194 (Sept. 23, 2011)

set of regulatory interventions was, as the FCC recently recognized, the creation of an "architecture" that "enables innovators to create and offer new applications and services without needing approval from any controlling entity, be it a network provider, equipment manufacturer, industry body, or government agency."[211] The FCC has even recognized that the emergence of intermediaries can "contribute to the marketplace discipline" of underlying telecommunications services in some contexts.[212] In essence, these interventions—grounded in maintaining a historical separation between those who create or cultivate data, services, and applications on the Internet and those who carry, transmit, or provide access to such data—created a stable architecture for higher-layer innovation by standardizing and commoditizing the essential inputs that Internet access providers offer to these higher layers.

The principle of network neutrality is, in part, intended to allow innovators and intermediaries to develop content and applications that rely upon the network effects of a supply of "Internetworked" users—that is, users who are undifferentiated at the network level—without needing to cut separate carriage deals with each of the access providers through which such users reach the Internet.[213] Network neutrality preserves the principle of a unified and interoperable network of networks, where a developer who wants to release a universally accessible service need not tailor that service to different networks.

If the principle of network neutrality were not in place, then a given application developer or intermediary would need to navigate a web of contractual undertakings on a variety of managed networks, and expose itself to the transaction costs and opportunities for holdup generated by the economic and technological differences between these networks. Each such agreement represents a point of control and an opportunity for carriers to extract additional tolls from, or place additional conditions upon, the prospective developer.[214] Carriers would be able to exert leverage via these points of control to lock users into proprietary versions of search, application, and content delivery services that were once universally shared. A world without network neutrality is a world where it is exceedingly unlikely that an under-funded or under-connected outsider could expect to draw in the number of users necessary to propagate now-

---

(to be codified in 47 C.F.R. pts. 0, 8).

211. Preserving the Open Internet, 76 Fed. Reg. at 59,194.

212. *Id.* at 59,218.

213. *See* Nicholas Bramble, Reply Comments, In the Matter of Preserving the Open Internet Broadband Industry Practices, GN 09-191 (Nov. 4, 2010).

214. *See* Jonathan Zittrain, *An Impenetrable Web of Fees*, N.Y. TIMES ROOM FOR DEBATE (Dec. 2, 2010, 7:20 AM), http://www.nytimes.com/roomfordebate/2010/8/9/who-gets-priority-on-the-web/an-impenetrable-web-of-fees.

ubiquitous services like Twitter, Skype, Pandora, Netflix, Wikipedia, Hulu, Google, or Facebook from scratch. Network neutrality, then, helps preserve the possibility that independent intermediaries and distributors will be able to compete effectively against the services offered by carriers.

But such structural interventions need to be coupled with investments in and broader thinking about the development of infrastructure if they are to preserve the basic ability of intermediaries to connect to universal networks.[215] Fortunately, one additional consequence of shifting governmental attention beyond the refinement of incentive schemes based on exclusive rights is that it frees up revenues for investment into infrastructure. Such investments can serve to shore up the basic safe harbor-driven regulatory strategy that this Article has been propounding. In exchange for additional governmental investment into the Internet's infrastructure, access and infrastructure providers can be required to refrain from interfering in competition among and innovation by higher-layer content, application, and search intermediaries.

2. Insufficient Protection of Users

At the same time, the destabilization wrought by § 512 and § 230, which this Article has generally celebrated, may generate additional destabilization of the context-specific protections that many users seek for their search, browsing, location, and communications activities.

A social network such as Facebook, for instance, grows as its users become more active and reveal more of themselves—their beliefs, their likes and dislikes, their locations, their constraints, their susceptibilities—to one another and to the network itself. Such data may be as valuable to advertisers as it is to friends browsing through an otherwise dull news feed, particularly (in both cases) when the data is non-intuitive.[216] Of course, many users would not, if asked outside the reciprocal sharing context of the social network, decide to release much of this non-intuitive data to the broader world. Facebook thus must rely upon the implicit

---

215. *See, e.g.*, Broadband Technology Opportunities Program, *About*, BroadbandUSA, http://www2.ntia.doc.gov/about ("The American Recovery and Reinvestment Act provided the Department of Commerce's National Telecommunications and Information Administration (NTIA) and the U.S. Department of Agriculture's Rural Utilities Service (RUS) with $7.2 billion to expand access to broadband services in the United States. Of those funds, the Act provided $4.7 billion to NTIA to support the deployment of broadband infrastructure, enhance and expand public computer centers, encourage sustainable adoption of broadband service, and develop and maintain a nationwide public map of broadband service capability and availability.").

216. Communications providers at lower layers may also seek to obtain access to such data. *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. Ill. L. Rev. 1417, 1420 ("Everything we say, hear, read, or do on the Internet first passes through ISP computers. If ISPs wanted, they could store it all, compiling a perfect transcript of our online lives.").

encouragement of friends to compel users to reveal data that these users would rather have left private or confined to a narrower context of distribution, or upon the explicit decision of friends to reveal data about a given user by referring to this user in their own posts. Such information-sharing norms may degrade users' preexisting expectations to be free from decontextualized or unwelcome or even defamatory speech, but this is part of the value proposition that Facebook offers both to users and to advertisers—*unexpected revelations of information* titillate users, encourage further revelations, and enable Facebook to serve contextual ads and build and export behavioral profiles based upon users' activity.

Similarly, in a world of exclusive licensing arrangements and powerful distribution channels, a new audio- or video-sharing website that wishes to challenge atrophied distribution channels often cannot rely solely on a strategy of obtaining licenses to the works being distributed on those channels.[217] One alternative strategy for an upstart distribution network seeking access to these works would be to rely on a compulsory licensing system, such as that contained in 17 U.S.C. § 114, which enables Internet radio stations such as Pandora to pay a judicially determined per-song fee instead of negotiating the rights to each song it plays.[218] But compulsory licenses are expensive, and are not available to all forms of distribution entities.[219] Furthermore, if an entity wishes to do more than enable passive listening to an algorithmically generated playlist based only in part upon occasional user input, and instead seeks to generate fine-grained user engagement with information on the website, the Internet radio model will not be well-tailored to this entity's goals. (Nor will direct infringement of existing rightsholders' copyrights be a real option for any law-abiding entity.) Instead, to some extent, the entity will again need to rely upon the implicit encouragement of friends to compel *users* to contribute information that will keep these friends and users coming back to the website.[220] Again, such information-sharing norms

217. *See* Michael Robertson, *Why Spotify Can Never Be Profitable: The Secret Demands of Record Labels*, GIGAOM (Dec. 11, 2011), http://gigaom.com/2011/12/11/why-spotify-can-never-be-profitable-the-secret-demands-of-record-labels; *see also* Tristan Louis, *Where the Hits Are Streaming in 2011*, TNL.NET (Jan. 14, 2012), http://www.tnl.net/blog/2012/01/14/internet-vod-2011-movies.

218. In particular, 17 U.S.C. §§ 114(d)(2)(C)(i) and 114(j)(13) (2006) enable providers to offer non-interactive transmissions of sound recordings so long as they satisfy various limitations including the number of songs played by the same artist within a three-hour time period. *See* DANIEL S. PARK ET AL., STREAMLINING MUSIC LICENSING TO FACILITATE DIGITAL MUSIC DELIVERY 6 n.33 (2011).

219. *See id*.; Ben Sisario, *Pandora and Spotify Rake in the Money and Then Send It off in Royalties*, N.Y. TIMES MEDIA DECODER BLOG (Aug. 24, 2012, 6:07 PM), http://mediadecoder.blogs.nytimes.com/2012/08/24/pandora-and-spotify-rake-in-the-money-and-then-send-it-off-in-royalties.

220. Contributions may take the form of original user contributions (e.g., *Charlie Bit My Finger*), user modifications of existing works (e.g., remixed versions of Rebecca Black's *Friday*), or user contributions of existing works (e.g., episodes of *The Colbert Report*).

may degrade rightsholders' preexisting expectations to be free from infringing speech and to tightly manage the distribution of their works, but this is part of the value proposition that a website such as YouTube offers both to users and to advertisers—*unexpected contributions of information* titillate users, encourage further contributions, and enable the website to serve contextual ads and build and export behavioral profiles based upon users' activity.

Other problems associated with the lack of legal requirements for intermediary responsibility arise in the context of online defamation, where new forums, particularly university- and high school-based gossip sites,[221] have enabled the proliferation of new and particularly damaging—because they are widely distributed and permanently enshrined—forms of defamation, bullying, and gender-based attacks.[222] It would be impossible to argue that there is no tension between the desire to promote a wide range of online discourse and the desire to protect those who are harmed by such discourse.[223] The question, however, is how to design a cure that addresses these harms without cutting off the positive externalities generated by online speech forums.

B. Preserving Space for Regulatory Intervention and Oversight in the Absence of a Single Pervasive Communications Framework

> What seemed like a hodgepodge eventually cohered into a whole.
>
> — Atul Gawande[224]

The overwhelming success of § 512 and § 230 points to a basic problem at the heart of Internet law. In short, the statutory provisions that Congress used to build out the core of the modern Internet are premised on the destabilization of other areas of the law and, in some cases, the outright elimination of pervasive legal frameworks for protecting certain values of privacy, safety, and security. Destabilization

---

221. *See, e.g.*, AutoAdmit, http://www.autoadmit.com (last visited Dec. 7, 2012); CollegeACB.co, http://www.collegeacb.co (last visited Dec. 7, 2012); the *Bored.at.[University Library]* series.

222. Danielle Citron has described "threats of sexual violence, doctored photographs of women being suffocated, postings of women's home addresses alongside the suggestion that they should be raped, and technological attacks that shut down feminist blogs and websites." Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 Mich. L. Rev. 373 (2009); *see* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. Rev. 61, 69–75 (2009); Nancy Kim, *Rhetoric, Norm Creation and the CDA*, Concurring Opinions (Apr. 15, 2009), http://www.concurringopinions.com/archives/2009/04/rhetoric_norm_c_1.html.

223. *See* Adam Thierer, *Dialogue: 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 (interviewing John Palfrey).

224. Atul Gawande, *Testing, Testing*, New Yorker (Dec. 14, 2009), http://www.newyorker.com/reporting/2009/12/14/091214fa_fact_gawande ("The government never took over agriculture, but the government didn't leave it alone, either. It shaped a feedback loop of experiment and learning and encouragement for farmers across the country.").

is here posed as an intentional strategy around which businesses and new models of data-sharing and distribution are built, and through which new forums for user expression come into being, but it can also be described as a disruptive force that eliminates the ability of users and rightsholders to rely on real-world expectations of privacy and safety.

The basic legal architecture that has allowed these websites to emerge—a model which refrains from requiring platform and network operators to take legal responsibility for the defamatory or infringing activities of users—leaves us in something of a strange position, then, when we turn toward thinking about how to encourage these intermediaries to take greater responsibility for the cultivation of safe, open, and secure communications environments. There are three basic strategies for attempting to promote such responsibility.

One strategy for protecting values of privacy and online safety is to outsource oversight over these values to private service providers, and then to hope that they protect these values reasonably well by applying some combination of their intrinsic interest in doing the right thing and their self-interest in avoiding more intrusive regulation. This is a simplified description of the last fifteen years of governmental involvement in the areas of privacy, safety, and online security.[225]

A second strategy is to fine-tune the various governmental interventions that, together, make up the Internet's legal architecture. At this point, limitations on secondary liability for violations of defamation and copyright law have largely been calibrated so as to enable the development of platforms for user-driven communications platforms.[226] But because they are premised on context-driven legal interventions rather than a universal order, these safe harbors can be further fine-tuned.[227] For example, legislators could recalibrate section 230 of the CDA in recognition of the greater potential archivability and searchability of defamatory communications that occurs online.[228] In the copyright

225. *See* FED. TRADE COMM'N, *supra* note 121, at 2 (describing the history of the notice-and-choice and harm-based models of privacy protection).

226. Such platforms for user-generated speech and information would be less likely to emerge if each platform manager were held responsible for the speech of its users. *See supra* Part III.B.

227. *See* YOCHAI BENKLER, *Law, Policy, and Cooperation*, *in* GOVERNMENT AND MARKETS: TOWARD A NEW THEORY OF REGULATION 299, 312–23 (Edward J. Balleisen & David A. Moss eds., 2011). Calibration of these levers need not take place at the level of the legal architecture itself. Instead, they can be implemented on a community-by-community basis.

228. *See* Danah Michele Boyd, Taken Out of Context: American Teen Sociality in Networked Publics (2008) (unpublished Ph.D. dissertation, University of California, Berkeley) (on file with author), *available at* http://www.danah.org/papers/TakenOutOfContext.pdf (defining properties central to the organization of "networked publics" including persistence, replicability, scalability, and searchability). Many have proposed adding features to § 230 to account for these different characteristics of online communications. *See, e.g.*, Nathaniel Gleicher, *Symposium: Legal Responses to Online Harassment*, CONCURRING OPINIONS (Apr. 14, 2009), http://www.concurringopinions.com/

context, legislators could fine-tune section 512 of the DMCA 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. Such design levers are more likely to be implemented when legislators approach information-production problems in a piecemeal rather than a systematic way,[229] given the variety of different motivations at stake in different communities.

Finally, this Part has suggested a third strategy for protecting values of online privacy and safety. The FCC, the FTC, and other regulatory and standard-setting bodies may be able to craft a series of pragmatic piecemeal interventions that would encourage greater public and private responsibility over the development of information-sharing tools and open infrastructures. These interventions would allow users to continue to share and access ideas, and would preserve the idea of the Internet as a source of diverse and antagonistic speech. For instance, online privacy itself can be modeled in architectural terms—as a common set of user expectations and design principles to which anyone is welcome to connect and build upon,[230] and as a necessary substrate within which different service providers and intermediaries must compete if they are to be fair participants within the marketplace for social networks and other services.[231] Online communities, in coordination with these regulatory bodies and private standard-setting bodies,[232] can develop clear rules regarding how open and transparent they will be with respect to their users and other communities and networks. And increasing the "exit options" for users of these services—for example, enabling them to remove their data from one service and import that data into a similar competing service—can also assist in the development of common standards and a common substrate that maintains architectural distinctions between the content layer, the intermediary layer, the network layer, and other surrounding layers.

---

archives/2009/04/ccr_symposium_l.html.

229. *See, e.g.*, Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d. 514, 519 (2d Cir. 2012) (quoting S. REP. NO. 105-190, at 19 (1998)). But "[r]ather than embarking upon a wholesale clarification" of various copyright doctrines, Congress elected "to leave current law in its evolving state and, instead, to create a series of 'safe harbors[]' for certain common activities of service providers." *Id.*

230. *See* LAWRENCE LESSIG, CODE VERSION 2.0, at 200–32 (2006); Crawford, *supra* note 207, at 389 ("[T]he Internet . . . can also provide a substrate that enables new ideas and new forms of social organisms to emerge, created by many different decisions to pay attention.").

231. *See* FED. TRADE COMM'N, *supra* note 121.

232. *See, e.g.*, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, http://www.icann.org (last visited Dec. 7, 2012); INTERNET ENGINEERING TASK FORCE, http://www.ietf.org (last visited Dec. 7, 2012); WORLD WIDE WEB CONSORTIUM, http://www.w3.org (last visited Dec. 7, 2012); *see also* Laura DeNardis, *The Emerging Field of Internet Governance* 7 (Yale Information Society Project Working Paper Series, 2010).

Success in implementing any of these legislative or regulatory strategies will likely be contingent upon how well governmental actors can tailor such interventions to the architectural model of earlier, layer-based regulations such as the Computer Inquiries and the safe harbors at issue in this Article.[233] If a proposed regulatory scheme or judicial remedy instead seeks to compress or eliminate the layers that have arisen between network infrastructure providers and content providers or entitlement holders—for example, by deputizing intermediaries to do the bidding of such providers—then it risks collapse of the same legal architecture that has generated the Internet's growth. The Stop Online Piracy Act and the Protect Intellectual Property Act were structured in a way that risked collapse of this layers principle; as a result, both bills faced significant resistance from the Internet community, and were tabled after heated legislative debate.

Successful implementation of the regulatory architecture described in this Article will also, of course, require telling more interesting stories about regulation and freedom on the Internet—stories that better enable us to see what sort of legal entity the Internet might be, and what it is capable of becoming. Given the architectural complexity of policy development, it may no longer be useful for legal scholars and other armchair empiricists to attempt to devise an optimal innovation policy that can be implemented by a single set of governmental actors. The relevant academic questions will instead concern how to allow these diffuse policy actors to work in conjunction (if not necessarily in concert) with one another, and more broadly how to set up numerous laboratories of innovation policy without granting to a single actor the power to determine how other actors implement those policies. This question can also be phrased as a question of how to create an *art* of governance that takes responsibility for the spread of mechanisms of governance beyond traditional regulatory centers.

CONCLUSION

While many have examined the destabilizing effect that section 230 of the CDA has had upon the clarity and enforceability of defamation law and that section 512 of the DMCA has had upon copyright law, this Article has investigated these processes of destabilization from several additional perspectives. First, it has given a detailed account of the development of safe harbors and immunities for Internet intermediaries, exploring what the growth of this form of legislation and regulation does to the standard incentive stories told by copyright law as well as broader justifications for governmental intervention into the production and

233. *See supra* Part V.A.1.

distribution of information. Second, this Article has examined how safe harbors and related telecommunications regulatory standards have set the conditions for the growth of a series of private intermediaries—search, application, audio, and video providers—that protect users by regulating the control and pricing power of content owners on the one hand and infrastructure owners on the other. And finally, it has examined where the rule of law might still fit into a system premised on the implementation of quasi-public regulations by private service providers.

It is now important, in light of the ongoing legislative debate over the copyright enforcement duties of intermediaries, to move beyond certain blank-slate assumptions associated with the legal structure of the Internet, and grapple in a more sustained way with the meaning of safe harbors, their consequences, and how they might be shaped into a more effective regulatory framework. If Congress declines to analyze the laws and system of regulations it is displacing, and instead presumes that it is writing a new rule in a place where previously there was no law, then its new rules will tend to cause a high degree of disruption to the marketplace that is currently in place. Without intermediaries in place to navigate the competing claims of access providers, media providers, and infrastructure owners, greater regulatory intervention may eventually be necessary. By overwriting the intermediary layer, legislators or regulators may inadvertently lay the groundwork for an Internet that is no longer self-sustaining. This Article, then, has sought to forestall that possibility by directing attention toward the articulation and preservation of the Internet's existing legal architecture.