

THE UNIVERSITY OF TEXAS SCHOOL OF LAW

Law and Economics Working Paper No. 045
April 2005



The Promise of Internet Intermediary Liability[†]

Ronald J. Mann* & Seth R. Belzley**

The University of Texas School of Law

This paper can be downloaded without charge from the
Social Science Research Network Electronic Paper Collection:
<http://ssrn.com/index.html>

An index to the working papers in
The University of Texas School of Law Working Paper Series
is located at <http://www.utexas.edu/law/>

[†] Forthcoming 47 WM. & MARY L. REV. (October 2005).

* Bruce W. Nichols Visiting Professor of Law, Harvard Law School, Ben H. and Kitty King Powell Chair in Business and Commercial Law, University of Texas School of Law. J.D. 1985 University of Texas. Co-Director, Center for Law, Business and Economics at the University of Texas. For comments on earlier drafts, we thank participants at a faculty workshop at the University of Texas School of Law and at the Internet Law Colloquium at Harvard's Berkman Center, Cam Barker, Doug Barnes, Oren Bracha, Nick Bunch, Arthur Cockfield, Assaf Hamdani, Doug Lichtman, Allison Mann, Travis Siebeneicher, Doron Teichman, and Jay Westbrook.

** J.D. 2005 University of Texas. Fellow, Center for Law, Business and Economics at the University of Texas, 2004–2005.

The Promise of Internet Intermediary Liability[†]

Ronald J. Mann^{*} & Seth R. Belzley^{**}

The internet has transformed the economics of communication, creating a spirited debate as to the proper role of federal, state, and international governments in regulating conduct that relates to or involves the internet. Many have argued that internet communications should be entirely self-regulated—either because they cannot or should not be the subject of government regulation. The advocates of that approach would prefer a no-regulation zone around internet communications, based for the most part on the unexamined view that internet activity is fundamentally different in a way that justifies broad regulatory exemption. At the same time, it is undisputed that some kinds of activity that the internet facilitates violate widely shared norms and legal rules. State legislatures motivated by those concerns have begun to respond with internet-specific laws directed at particular contexts, giving little or no credence to the claims that the internet needs special treatment.

This Essay starts from the realist assumption that government regulation of the internet is inevitable. Thus, instead of focusing on the naïve question of whether the internet should be regulated, it discusses how to regulate internet-related activity in a way that is consistent with approaches to analogous offline conduct. The Essay also assumes that the most salient characteristic of the internet is that it inserts intermediaries into relationships that could be, and previously would have been, conducted directly in an offline environment. Existing liability schemes generally join traditional fault-based liability rules to broad internet-specific liability exemptions. Those exemptions are supported by the premise that in many cases the conduct of the intermediaries is so wholly passive as to make liability inappropriate. As time has gone on, this has produced a great volume of litigation, mostly in the context of the piracy of copyrighted works, in which the responsibility of the intermediary generally turns on fault, as measured by the level of involvement of the intermediary in the challenged conduct.

We argue that the pervasive role of intermediaries calls not for a broad scheme of exoneration, premised on passivity, but rather for a more thoughtful development of principles for determining when and how it makes economic sense to allocate responsibility for wrongful conduct to the least cost avoider. The rise of the internet has brought about three changes that make it more likely that intermediaries will be least cost avoiders in the internet context than they previously have been in offline contexts: an increase in the likelihood that it will be easy to identify specific intermediaries for large classes of transactions; a reduction in the information costs that make it easier for the intermediaries to monitor the conduct of end-users; and the anonymity that the internet fosters makes remedies against end-users generally less effective. Accordingly, in cases in which it is feasible for intermediaries to control the conduct, we recommend serious attention to the possibility of one of a series of three different schemes of intermediary liability: traditional liability for damages; takedown

[†] Forthcoming 47 WM. & MARY L. REV. (October 2005).

^{*} Bruce W. Nichols Visiting Professor of Law, Harvard Law School, Ben H. and Kitty King Powell Chair in Business and Commercial Law, University of Texas School of Law. J.D. 1985 University of Texas. Co-Director, Center for Law, Business and Economics at the University of Texas. For comments on earlier drafts, we thank participants at a faculty workshop at the University of Texas School of Law and at the Internet Law Colloquium at Harvard's Berkman Center, Cam Barker, Doug Barnes, Oren Bracha, Nick Bunch, Arthur Cockfield, Assaf Hamdani, Doug Lichtman, Allison Mann, Travis Siebeneicher, Doron Teichman, and Jay Westbrook.

^{**} J.D. 2005 University of Texas. Fellow, Center for Law, Business and Economics at the University of Texas, 2004–2005.

schemes (in which the intermediary must remove offensive content upon proper notice); and “hot list” schemes (in which the intermediary must avoid facilitation of transactions with certain parties).

The final Part of the Essay uses that framework to analyze the propriety of intermediary liability for several kinds of internet-related misconduct. We are agnostic about the propriety of any particular regulatory scheme, recognizing the technological and contextual contingency of any specific proposal. Because any such scheme will impose costs on innocent end-users, the selection of a particular level of regulation should depend on the policymaker’s view of the net social benefits of eradication of the misconduct, taking into account the costs of compliance with the regulation by the intermediaries and innocent users. Still, our analysis suggests three points. First, the practicality of peer-to-peer distribution networks for the activity in question is an important consideration, because those networks undermine the effectiveness of the regulatory scheme, making regulation less useful. Second, the highly-concentrated market structure of Internet payment intermediaries makes reliance on payment intermediaries particularly effective as a regulatory strategy because it is difficult for illicit actors to relocate to new payment vehicles. Third, with respect to security harms (viruses, spam, phishing, hacking, and the like), we conclude that the addition of intermediary liability in those cases is less likely to be beneficial, because market incentives appear to be causing substantial efforts by intermediaries to solve these problems even without the threat of liability.

I.	Introduction	2
II.	The Internet and Misconduct.....	9
	A. The End-to-End Structure of the Internet	9
	B. Internet Actors	10
	1. Primary Malfeasors	10
	2. Internet Intermediaries	11
	C. Existing (Fault-Based) Liability Schemes	14
III.	Liability Without Fault: Internet Intermediaries as Gatekeepers	19
	A. The Basic Premise	19
	1. The Nature of Gatekeeper Liability.....	19
	2. Gatekeeper Liability and the Internet.....	21
	B. Variations on the Theme	22
	C. A Framework for Analysis	24
IV.	Applications to Specific Types of Conduct.....	27
	A. Dissemination of Content.....	27
	1. Trafficking in Contraband and Counterfeit Products	27
	2. Internet Gambling	31
	3. Child Pornography	39
	4. Internet Piracy	45
	B. Breaches of Security.....	47
	1. Lack of Strong Intermediaries.....	47
	2. Market Incentives Already Exist.....	49
V.	Conclusion.....	50

I. Introduction

To think about the role of law in electronic commerce is to consider the balance between government regulation and freedom of action in the private sector. Juxtaposing that balance with the commercialization of the internet in 1994 and its rapid growth since that date presents an

unusually dynamic policy problem. In her book *Ruling the Waves*, Debora Spar portrays the problem aptly, arguing that society's reactions to important discoveries follow a cyclical historical pattern.¹ Using examples that start with the 15th century reign of Prince Henry the Navigator of Portugal and continue through the rise of the internet in the 20th century, she discerns four phases through which the society that exploits those discoveries commonly passes: innovation, commercialization, creative anarchy, and rules.² The phase of innovation is the flash point of discovery—Morse's invention of the telegraph, for example.³ The phase of commercialization is the phase in which pioneers (or pirates, depending on your perspective) move into the new area seeking to exploit its potential: one of Spar's examples discusses the actual pirates who exploited the newly discovered Atlantic in the 16th century.⁴ The phase of creative anarchy is the phase when the needs of ordinary commerce come into tension with the theretofore-freewheeling spirit of the new frontier.⁵ Spar's best example of that phase is the 1920's era of radio broadcasting, when competing (and wholly unregulated) radio stations broadcast on overlapping frequencies that made it difficult for any of them to be heard by listeners.⁶ The final phase—rules—follows ineluctably as the commercial enterprises unable to suppress anarchy on their own call for government intervention as the best vehicle for bringing order (and profit) to the wild frontier.⁷

Using that framework, the internet is in the midst of the third phase. There are numerous examples of early actors whose businesses have provided a major impetus for the growth of the internet, as we know it. There also are a set of legal rules that have granted those actors broad freedom of action or exempted them from rules that govern analogous conduct outside cyberspace. Consider, for example, the immunity granted internet service providers by the Communications Decency Act⁸ and the Digital Millennium Copyright Act,⁹ the protection from

1. DEBORA L. SPAR, *RULING THE WAVES: CYCLES OF DISCOVERY, CHAOS, AND WEALTH FROM THE COMPASS TO THE INTERNET* 11 (2001).

2. *Id.* (“[L]ife along the technological frontier moves through four distinct phases: innovation, commercialization, creative anarchy, and rules.”).

3. *Id.* at 11–12.

4. *Id.* at 12–15.

5. *Id.* at 15–18.

6. *Id.* at 157–58.

7. *Id.* at 18–22.

8. 47 U.S.C. § 230(c)(1) (2004) (making certain requirements of the CDA inapplicable to ISPs).

9. 17 U.S.C. § 512 (2004).

new taxation granted by the Internet Tax Freedom Act,¹⁰ the rise of unregulated peer-to-peer music sharing, and the lack of regulation of person-to-person payment providers.

Each of those instances, however, has been associated with a growing backlash of pressure, as parties who perceive that they are disadvantaged by those exemptions seek the establishment of more rigorous regulatory regimes. That backlash is a primary indication that an industry has developed to the point where regulation is appropriate. This Essay considers how to implement regulatory regimes that are better suited for the internet context.¹¹ The basic problem is that although the internet undeniably has brought increased efficiency to American firms, eased communication among distant friends, and changed the way we shop, book travel, entertain and are entertained, it also affords the same ease of communication, increased efficiency, and, importantly, anonymity for those who prefer to use those advantages to violate the law. Legal reactions to one pervasive violation—internet-based piracy of copyrighted works—have been especially vigorous, perhaps because that activity poses a serious threat to an entrenched industry scared of losing its grasp over its only asset—copyrighted works. Countless numbers of pages in reporters and law reviews have been devoted to finding ways to prevent internet piracy. Nevertheless, internet piracy continues and promises to recover from its recent dip¹² as software developers and users adapt and evolve to avoid the current attempts of the legal regime to control their activities.

Piracy is not our focus, in part because of our view that eradication of piracy would require an exercise more in the vein of social engineering than of legal reform.¹³ Rather, our focus is a

10. Pub. L. No. 105-277, tit. 9, 112 Stat. 2681, 2719–26 (1998). This moratorium on taxing internet access has been extended twice since its original enactment, most recently in November 2004 as the Internet Tax Nondiscrimination Act, thus preventing taxation on internet access through at least October 2007. See *U.S. House Clears Tax Ban on Internet Service*, WALL ST. J., Nov. 22, 2004, at A7; *Bush Signs IDEA, Internet Tax Bills*, CONGRESS DAILY, Dec. 3, 2004, at 8. For general discussion, see Arthur Cockfield, *Designing Tax Policy for the Digital Biosphere: How the Internet is Changing Tax Laws*, 34 CONN. L. REV. 333, 363-65 (2002).

11. Of course, the first question in each instance is why the businesses that are harmed cannot solve the problems on their own. For example, why should the government regulate unsolicited commercial e-mail—however annoying it might be—given the obvious market pressures spurring the major internet service providers to disable those that send it? That question motivates the skepticism we express about such regulation in subpart IV(B).

12. In fact, some industry experts suggest that the efficacy of RIAA lawsuits is really short-lived. See Carolyn Said, *Studios to Sue Pirates. Film Industry Fights Illegal File Sharing*, S.F. CHRON. Nov. 5, 2004, at C1 (“‘When the RIAA has filed a bunch of lawsuits, we’ve seen a decrease in file sharing for a month to a month and a half; then it comes back up again,’ said Jim Graham, a spokesman for BayTSP of Los Gatos, which tracks files offered online for sharing.”). But there is also evidence that lawsuits are effecting long-term successes in some cases. See *File-Sharing Website Ceases Operation*, L.A. TIMES, Dec. 21, 2004, at C3 (reporting that entire websites that provided links to make a popular file-sharing program called BitTorrent operate were completely shutting down after lawsuits were filed). It remains to be seen, however, if the BitTorrent system will recover from this setback. Such a recovery seems likely given the popularity of the program and the ease of locating the simple and necessary websites out of the reach of such lawsuits.

13. Many would argue that this is a case where the underlying business models must shift to meet the limitations of the regulatory regime. Indeed, there is reason to believe that there is substantial upside to the business models that the internet facilitates. See Chris Anderson, *The Long Tail*, WIRED, Oct. 2004, available at <http://www.wired.com/wired/archive/12.10/tail.html> (last visited Mar. 25, 2005) (describing how the ability to offer broader product offerings gives electronic

number of other common uses of the internet for unlawful purposes that have attracted much less attention. For example, each day gamblers physically present in jurisdictions that outlaw gambling bet millions of dollars on card games and sports matches. Although the use of the internet does not affect the illegality of that gambling, little has been done to curtail the activity. Further, the internet has made the balance between regulating socially unacceptable forms of speech and violating the First Amendment even more difficult, leading to the proliferation of material such as child pornography. Similarly, the anonymity that the internet fosters has made it much easier to buy and sell counterfeit goods, pharmaceuticals not lawfully available in the jurisdiction of purchase, and other forms of contraband. Each year Americans spend billions of dollars and millions of hours combating computer viruses spread over the internet.¹⁴

Thus, although the internet has improved our lives in dozens of ways, it has also brought detrimental behavior that has proved hard to constrain. Controlling that conduct without restraining the potential of the internet surely is a worthy goal. This Essay suggests that the impulse to respond to those problems inevitably depends on internet intermediaries—chiefly internet service providers (ISPs), payment intermediaries (PIs), and auction intermediaries (most prominently, eBay). Although a traditional focus on the underlying wrongful conduct would view the intermediary as a passive conduit exempt from normative responsibility for the activity of parties that use its system,¹⁵ direct regulation of the responsible parties is often impractical. Where the principal difficulty for analogous offline misconduct is the common lack of financial responsibility by the offenders, the rise of the internet presents regulators with new challenges by making it easier for illicit actors to conceal their identity and to locate themselves in jurisdictions beyond the reach or influence of law enforcement officials inside the United States.

Yet internet intermediaries often fill critical roles in the illicit behavior that frustrates regulators. Indeed, internet intermediaries often profit directly from transactions that would be effectively banned in the offline environment. Policymakers of course have not been blind to the possibility of employing internet intermediaries to control misconduct of their customers. As early as 1995 a task force created by President Clinton suggested imposing strict liability on ISPs

commerce merchants the ability to extract profits from books, music, and movies that could not profit in an offline retail environment); JOHN ALDERMAN, *SONIC BOOM: NAPSTER, MP3, AND THE NEW PIONEERS OF MUSIC* (2001).

14. One estimate put the total cost of viruses at \$55 billion for 2003. *Compressed Data*, TORONTO STAR, Jan. 17, 2004, at Business (“Trend Micro Inc., the world’s third-largest anti-virus software maker, said yesterday computer virus attacks cost global businesses an estimated \$55 billion (U.S.) in damages in 2003, a sum that would rise this year.”).

15. For an emphatic statement of that perspective, see *Doe v. GTE Corp.*, 347 F.3d 655, 658-59 (7th Cir. 2003) (per Easterbrook, J.).

as a means for controlling some of the dangers of the internet.¹⁶ More recently, state attorneys general and the ATF reached an agreement with major credit card companies to prevent the processing of payments for illegal Internet cigarette sales.¹⁷ Similar initiatives have been proposed in Congress to address the problem of online sales of prescription drugs.¹⁸ And, Pennsylvania passed a statute (since held unconstitutional) that would have required ISPs to block access to child pornography sites.¹⁹ Private parties have pursued intermediaries under principles of tort law. In recent suits against, for example, Grokster²⁰ and Ebay,²¹ plaintiffs have directed their attention to internet intermediaries in trying to curtail conduct that has detrimental effects on their businesses.

Thus far, however, the law has been unable to respond in a way that effectively regulates the activity of the intermediaries. On the contrary, as discussed above, to the extent Congress has acted to address the question, the laws have been designed to insulate the intermediaries from liability.²² State regulators have been considerably more aggressive, but, as we discuss, much of the existing formal legislative activity has fallen in the face of litigation,²³ and the problems of coordinating efforts among multiple jurisdictions have imposed difficulties in others.²⁴ We hope that our focus here on the costs and benefits of regulation can guide regulators in developing more nuanced and context-specific rules more likely to withstand judicial attack. Recognizing

16. See RONALD H. BROWN & BRUCE A. LEHMAN, INFO. INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 114–24 (1995) (discussing the arguments for and against carving out an exception to the general rule of vicarious liability in copyright infringement for ISPs and rejecting such an approach), available at <http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf>.

17. See *Deal Aims to Prevent Web Cigarette Sales*, N.Y. TIMES, Mar. 18, 2005, at Business; <http://www.atf.gov/press/fy05press/031705internetcigsalesinitiative.htm>.

18. See Gilbert M. Gaul & Mary Pat Flaherty, *Google to Limit Some Drug Ads*, WASHINGTON POST, Dec. 1, 2003, available at <http://www.washingtonpost.com/wp-dyn/articles/A23588-2003Nov30.html> (last visited Mar. 25, 2005).

19. See *infra* notes 172–187.

20. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 380 F.3d 1154 (9th Cir.) (refusing to find liability for Grokster even though it aided end-users in copyright infringement because the service was fundamentally different than Napster), *cert. granted*, 125 S. Ct. 686 (2004).

21. *Hendrickson v. Ebay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (finding that eBay was protected under §512(c)(3) of the Digital Millennium Copyright Act for assisting in the sale of infringing material when notice of the infringement was not specific enough).

22. Joel Reidenberg in particular has emphasized the incongruity of Congress's preference for broad statutory exemptions coupled with the facility with which intermediaries could address *some* of the most salient problems. See Joel Reidenberg, *States and Internet Enforcement*, 1 UNIV. OTTAWA L. & TECH. J. 1 (2004) (noting the early exemptions for internet intermediaries and the need to look for enforcement mechanisms directed at intermediaries).

23. The most salient example is *Center for Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 620 (E.D. Pa. 2004) (invalidating a Pennsylvania statute targeting intermediaries in an effort to limit access to adult content). A fair assessment of that litigation is that excessively aggressive and insensitive enforcement by state regulators led to the demise of a regulatory initiative that might have survived had it been implemented with a more guarded attitude.

24. Compare, for example, the relative success states have had in regulating cigarette sales (see *supra* note 17) with the persistent difficulty that Massachusetts has encountered in enforcing its unusual (though plainly legitimate) weapons law. See *AG Reilly Obtains Court Order Prohibiting Online Sales by Weapons Dealers* (Sept. 10, 2004 press release discussing repeated lawsuits directed at online weapons dealers).

the differing constituencies and aims of state and federal regulators,²⁵ it is our hope that our analysis can help to facilitate the cooperation of federal authorities that will be necessary to provide effective solutions to the problems motivating existing state initiatives. At the same time, we want to illuminate the just concerns of technologists trying to preserve the generative potential of the internet, with a view to facilitating intervention that is more sensitive and less blunt.²⁶ Thus, among other things, our analysis evinces a general preference for initiatives that grant safe harbors to intermediaries in response to specifically defined conduct rather than general imposition of liability.²⁷

Scholars have followed up on those possibilities in a variety of ways. Doug Lichtman, for example, has argued in papers with Bill Landes and Eric Posner that traditional principles of tort law properly can be used to impose a greater level of responsibility on intermediaries.²⁸ Although we are sympathetic with much of his analysis, our work takes a different tack, because we largely jettison the traditional tort principles on which he builds. In our view, the normative underpinnings of traditional tort law are not as useful a device for establishing appropriate standards of conduct as the more direct and contextual focus on the costs and benefits of intermediary liability that we propose. As we illustrate, a focus on traditional tort law notions of fault necessarily diverts attention to subjective normative questions of blame and responsibility that more properly should focus on questions of effective regulatory design.

Other scholars have considered the possibility that intermediaries might be the least-cost avoiders of some forms of internet-related misconduct. Assaf Hamdani, for example, discusses a number of problems with imposing strict liability on ISPs for cyberwrongs.²⁹ Similarly, Kumar Katyal's work on cybercrimes discusses the possibility of imposing liability on ISPs as a

25. For a parallel emphasis on the differing perspectives of state and federal regulators attending to corporate governance, see Mark J. Roe, *Delaware's Politics*, 118 HARV. L. REV. (forthcoming 2005).

26. For general discussion of the risks of unduly intrusive intervention, see Jonathan Zittrain, *The Future of the Internet—and How to Save It* (unpublished 2005 manuscript) (on file with author). For a few current examples, see Katie Dean, *Techies Blast Induce Act*, Wired, July 23, 2004, at http://www.wired.com/news/politics/0,1283,64315,00.html?tw=wn_tophead_2 (last visited Mar. 25, 2004) (discussing the proposed Inducing Infringements of Copyright Act, S. 2560, 108th Cong., 2d Sess. (2004), which would impose liability on manufacturers of devices that “induce” users to engage in illegal filesharing); Michael Geist, *Say No to Big Brother Plan for Internet*, TORONTO STAR, Mar. 7, 2005 (decrying Canada's proposed “lawful access” initiative, which would require all ISPs to facilitate real-time interception of internet communications).

27. The National Association of Attorneys General, for example, has called for granting states a right of action in federal courts to obtain nationwide injunctive relief against intermediaries to stop unlicensed online pharmacies. See *Kansas Attorney General Carla Stovall Testifies On Illegal Online Pharmacies, State-Federal Cooperation to Protect Consumer* (undated press release), available at http://www.naag.org/legislation/stovall_online_pharm.php (last visited Mar. 25, 2005). More recent efforts against intermediaries (see note 18, *supra*) presage analogous legislative initiatives against the intermediaries.

28. DOUG LICHTMAN & ERIC POSNER, HOLDING INTERNET SERVICE PROVIDERS ACCOUNTABLE 3 (U. Chi. L. & Econ., Olin Working Paper No. 217, July 2004, available at <http://www.ssrn.com/abstract=573502>) (arguing for liability that forces such cooperation); William Landes & Douglas Lichtman, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395 (2003).

29. Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901 (2002).

response.³⁰ Generally, however, that literature has failed to understand the way in which the tailoring of remedies to particular contexts can alter or remove so many of the most salient and powerful problems with intermediary liability generally. For example, Hamdani provides a detailed analysis of the considerations that justify a choice between strict and negligence-based liability for gatekeepers, but his framework suggests that there should be no gatekeeper liability at all in cases in which a damages regime is too costly.³¹ As we explain below, there are other operationally less-intrusive regulatory alternatives (takedown regimes and hot-list schemes) that in many contexts might vitiate the costs that justifiably concern him. Similarly, Katyal's discussion—perceptive as far as it goes—is focused on the idea that principles of “due care” should guide regulation of intermediaries.³² He does not recognize that effective regulation of intermediaries must leave concepts of due care behind.

In sum, the basic thesis of this Essay is that the time has come for the internet to grow up, for Congress and for 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. Part two of the Essay sets the stage by describing the technological structure of the internet, the actors that serve as intermediaries, and the existing (largely fault-based) liability regimes. Part three describes our proposal, which rests entirely on the economic principle of identifying the least-cost avoider. We present a consciously exceptionalist³³ argument, that specific characteristics of the internet make intermediary liability relatively more attractive than it has been in traditional offline contexts: the ease of identifying intermediaries; the relative ease of intermediary monitoring of end-users; and the relative difficulty of direct regulation of the conduct of end-users. We then discuss the circumstances when intermediary liability will be practical, and the characteristics that differentiate the desirability of three different regimes of liability: traditional damages regimes; takedown regimes (in which offensive content must be removed after proper notice); and “hot list” regimes (in which the intermediary must avoid facilitation of transactions with certain parties). Finally, Part four of the Essay applies our

30. Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1095–1101 (2001). For a similar discussion of internet gambling, see Jonathan Gottfried, *The Federal Framework for Internet Gambling*, 10 RICH. J.L. & TECH. 26, *74–*91 (2004).

31. The closest Hamdani comes to considering alternative regimes is a brief passage suggesting that legislators might impose specific monitoring standards instead of damages liability. Hamdani, *supra* note 29, at 934–35.

32. Katyal, *supra* note 30, at 1095–1101.

33. Although our argument does lead us to suggest special rules for the internet, we hope that our effort in subpart III(A) to ground our rules in specific features of the internet justifies those differences. As the discussion below should make clear, we generally are much more sympathetic to the view (advanced most forcefully by Jack Goldsmith in work such as *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998)) that traditional principles of regulatory analysis are adequate to respond to the special features of the internet. Indeed, a principal motivation for this Essay is the view that the existing internet-based exceptions from liability go much too far in protecting conduct that would be unlawful in more conventional contexts.

proposal to four types of content harms discussed above (contraband, gambling, child pornography, and piracy) and to the general category of security harms. Although previous writers have discussed at great length the pros and cons of imposing liability on intermediaries related to piracy, there has been relatively little attention to the role intermediaries can play in other contexts, and almost no attention to the specific features of intermediaries and their particular businesses that make regulation in particular contexts more and less effective.

II. The Internet and Misconduct

A. *The End-to-End Structure of the Internet*

The internet is essentially a series of computers connected through a complex system of cables. The internet was originally conceived of and designed by the United States government for use by the military and university researchers.³⁴ When the internet was confined to use exclusively by the military, the military itself, military contractors, or university researchers managed connections between computers. But as the internet was adapted to use by the general public, private companies emerged that provided the links between private computers connected to the internet.³⁵

Today, the internet is a network of privately owned networks that communicate using a common computer language called Transfer Control Protocol/Internet Protocol (TCP/IP).³⁶ When an internet user requests data over the internet, his request is routed first from his computer to the network to which his computer is connected, then across lines to the network to which the computer holding the requested content is connected, and finally to the computer that contains the requested content. These separate networks comprising the internet could be operated using any number of different transfer languages. The structure of the internet and the common use of TCP/IP for transfer between networks allow all of these different networks to communicate with each other. Larry Lessig has described this structure of the internet as utilizing an end-to-end principle that places the intelligence of the network at the end of unintelligent conduits, thus allowing the network to easily evolve and adapt to changing and improving technology.³⁷ Lessig

34. See generally JANET ABBATE, *INVENTING THE INTERNET* 36 (MIT Press 1999) (describing the creation of packet switching and the interlinking of distant computers during the 1960s and 1970s by the Advanced Research Projects Administration, a division of the Department of Defense).

35. See *id.* at 183–218.

36. Lawrence B. Solum and Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 821 (2004).

37. LAWRENCE LESSIG, *THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD* 34 (2001). Although Lessig did not originally conceive of the E2E principle, he has locked onto the idea and eloquently suggested the logical implications of the internet structure for internet regulations.

suggests that this design has strong implications for—even dictates—the appropriate types of internet regulations.³⁸ We agree with Lessig that regulations that compromise the end-to-end structure of the internet must be recognized as imposing a cost by restricting future innovations in internet applications. But rather than viewing the end-to-end principle as inviolate, we believe that it is sufficient simply to recognize the costs of intrusive regulations in a larger cost-benefit analysis.³⁹

B. *Internet Actors*

While previous scholars have built on Lessig’s insight by breaking the internet down into various layers that might be regulated in different ways,⁴⁰ we take the key point to be a recognition that the bulk of the regulable activity is likely to occur at the ends of transmissions, rather than in the center. This does not mean, however, that the parties to internet transmissions interact with a featureless black box that is beyond the reach of law or regulatory initiative.⁴¹ Rather, the implication is that a sensible regulatory framework must start with an understanding of the different kinds of actors that are situated at the endpoints of internet transmissions, acting to facilitate the actions of end-users sending, requesting, and receiving those transmissions. The sections that follow provide a crude taxonomy.

1. *Primary Malfeasors.*—Primary malfeasors offer or receive content or products over the internet that violates laws related to subjects such as copyright, child pornography, gambling, and trademarks. The proprietor of a gambling website, for example, offers content over the internet that allows visitors to violate gambling laws. On the other side of the transaction, visitors to a gambling website receive content and interact with the content in ways that violate gambling laws. Likewise, a person who introduces a malicious internet worm onto a network operates at the content layer by putting content onto the web that threatens all computers with internet access.

38. See, e.g., Mark A. Lemley and Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925 (2001) (arguing that the E2E principle suggests that cable broadband internet service providers should not be allowed to force customers to subscribe to particular content in order to receive internet service).

39. For a similar intuition, see Zittrain, *supra* note 26. Canadian regulators have in fact determined that violating the end-to-end principle is justified by the need for regulating internet conduct. The “lawful access” initiative would require ISPs and future communications providers to design their networks so that they can collect data about customers and intercept transmissions when required to do so by lawmakers. Michael Geist, *Do We Want Fee-Based, Surveillance-Ready Web? Say No to Big Brother Plan for Internet*, TORONTO STAR, Mar. 7, 2005, at D01. For general information on the Canadian initiative, see NEVIS CONSULTING GROUP, SUMMARY OF SUBMISSIONS TO THE LAWFUL ACCESS CONSULTATION (Apr. 2003), available at http://canada.justice.gc.ca/en/cons/la_al/summary/las_report_042803_e.pdf.

40. E.g., Solum & Chung, *supra* note 36; Kevin Werbach, *A Layered Model for Internet Policy*, 1 J. Telecomm. & High Tech. L. 37, 59 (2002).

41. Again, consider the Canadian “Lawful Access” initiative. See *supra* note 40.

2. *Internet Intermediaries.*—The early days of the internet witnessed many broad claims about how the internet would lead to widespread disintermediation,⁴² as transacting parties gained the ability to deal directly with each other. The reality, however, has been precisely the contrary. At a basic level, the technology of the internet requires the insertion of intermediaries between interacting parties in two ways. First, for all interactions over the internet, the communication necessarily involves the internet itself, as well as the parties necessary to facilitate the particular communication (except for those relatively few entities sufficiently involved in internet transmissions to be directly connected to each other). More importantly for our purposes, commercial interactions on the internet require the use of other intermediaries, chiefly payment intermediaries and auction intermediaries, because those transactions cannot use cash as payment and because there must be some method of bringing the parties together, with auction sites providing a successful vehicle for internet interaction. We cannot hope to describe *all* of the intermediaries that facilitate internet commerce in the current environment, much less those that will arise in the years to come. For present purposes, however, it is useful to focus on three classes of businesses, which in our view include the most prevalent and interesting types of intermediaries: ISPs, Payment Intermediaries, and Auction Intermediaries.

a. *ISPs.*—ISPs are necessary at every stage of an internet transaction.⁴³ To end-users, the ISP is the entity responsible for making access to the content on the internet possible. An end-user is not concerned with which company actually provides the physical network that transmits data across the country or the protocols that ensure that the data gets routed to the right place. But recognizing the importance to appropriate regulatory design of sensitivity to context, it is important to distinguish different roles that ISPs play in common internet activities.

For our purposes, it is useful to distinguish three distinct roles that ISPs might play in an internet transaction: *Backbone Providers*, *Source ISPs*, and *Destination ISPs*. The first group includes those that operate solely at the level of transmission (*Backbone Providers*), with no direct relationship to any of the actors at the endpoints of the transmission. For our purposes,

42. E.g., Andrew L. Shapiro, *Digital Middlemen and the Architecture of Electronic Commerce*, 24 OHIO N.U. L. REV. 795 (1998).

43. As Jonathan Bick explains:

Even the simplest internet transaction usually involves a user's computer, an internet service provider's access computer, a regional router, a governmental backbone computer, another regional router, another internet service provider's computer, and a content provider's computer. So, even in the simplest transactions, there are many more intermediaries than users or content providers.

Jonathan D. Bick, *Why Should the Internet Be Any Different?*, 19 PACE L. REV. 41, 63 (1998).

backbone providers are of relatively little interest, because of the costs and difficulties involved in configuring their networks to distinguish between different types of data they are carrying.⁴⁴

Destination ISPs serve the end-user who requests content over the internet. Those ISPs are the entities that bill the end-user for Internet service and provides applications such as the ability to connect to the World Wide Web. Thus, they serve as gateways for end-users to everything on the internet. As the owners of equipment that operates to link networks to the internet backbone, and translate application data into a format that can be transmitted along the backbone, these ISPs are well-placed to block access to data available on the internet or to prevent the transfer of harmful data (worms, viruses, spam, etc.).

One premise of this Essay is that the inability of the current regime to control many of the harms of the internet comes from a myopic focus on the *Source ISP*, the provider that provides access to the business at which the unlawful content is made available.⁴⁵ For regulatory purposes, there are two important distinctions between the Destination ISP and the Source ISP. The first is a substantive one: the Destination ISP serving ordinary end-users is most unlikely to have any direct involvement with or specific knowledge regarding the primary malfeasor. The Source ISP, in contrast, may be involved in a range of ways that are relevant both in assessing how “fair” it is to “blame” the Source ISP for the misconduct (the predominant question in existing judicial doctrine) and also in assessing how effectively the Source ISP could serve as a gatekeeper to stop the misconduct (the predominant question for us). For example, a Source ISP that is providing not only access, but also a server on which the unlawful material resides, may be much better placed to monitor and control the activity than one that provides only access.

The second distinction, however, is the one of importance for our project: the Destination ISP that wishes to serve ordinary end-users cannot readily remove itself from the jurisdiction of the government in whose territory the users are located. By contrast, the Source ISP that is willing to facilitate unlawful behavior can remove itself to a jurisdiction that does not prohibit the behavior in question. Thus, for example, the Source ISP that is willing to facilitate internet

44. This, at least, seems to be the view of earlier writers, who argue that the difficulty of understanding the data that travels over ISP networks is an artifact of the internet’s basic transmission protocol, under which the data that travels over those networks is in the forms of dis-integrated packets of any particular file. See Lessig, *supra* note 37, at 34; Solum & Chung, *supra* note 36, at 829. Commenters on this paper, however, suggest that this perspective is overstated. For one thing, it seems plain that backbone providers readily can discern the IP address to which packets are being routed. More generally, more than one reader of a draft of this essay has found it easy to imagine technology that would allow backbone providers to recognize certain types of content passing through its network. As with much of the analysis in this paper, changes in technology might change the optimal regulatory strategy. It seems to us, however, that regulation at the backbone level is likely in most cases to involve costs to *all* traffic that would outweigh the benefits reasonably attributed to the regulation. See Zittrain, *supra* note 26.

45. This point is best made by Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003).

casinos can make its services available anywhere that local laws allow such activities,⁴⁶ putting these entities outside the reach of most law enforcement agencies.⁴⁷ But the Destination ISP that provides the connection for customers in Ohio to visit the internet casino in Antigua must be present in Ohio, if only in the form of a local server, cable, or router.

b. Payment Intermediaries.—Payment intermediaries facilitate the transfer of funds between parties to internet transactions. Because most internet transactions do not involve face-to-face interactions between the transacting parties, some intermediary ordinarily must be enlisted to make it practical for a buyer to transfer funds to a seller in a reliable way. For example, when a person using the internet incurs a debt, either by shopping on the internet or visiting sites that charge fees for activities conducted at the website, payment intermediaries are involved in the chain of events required for the transaction to be consummated. Thus, if A visits a gambling website whose servers are located in Antigua and signs up for an account so that he can participate in a game of internet poker, A must provide the website some form of security to ensure that any gambling debts incurred will be paid. Often, a website will simply require a credit card to be on file. Alternatively, the site may use A's bank to transfer money in advance or otherwise to secure some assurance that A's potential gambling losses will be covered. The credit card company or the bank in practice is a necessary actor for the conduct in which A wants to engage.

Our regulatory analysis depends heavily on particular features of existing internet payment intermediaries. Most importantly, the market is highly concentrated in the hands of the dominant credit card networks, and new entrants face high—perhaps insuperable—barriers to entry.⁴⁸ Intermediaries that have such a comprehensive command of the market at some point begin to resemble the common carriers on whom lawmakers commonly have imposed regulatory obligations in the public interest. To be sure, early predictions that a new kind of money—generically called electronic money—would be created to facilitate internet transactions. Still,

46. In such a structure, there is and has been an international race to the bottom to attract business to certain countries by decreasing the legal obstacles to their establishment. In the context of internet gambling, the winner of this race has arguably been the small island of Antigua in the British West Indies. See Don Yaeger, *Bucking the Odds*, SPORTS ILLUSTRATED, Jan. 8, 2001, at 26 (“Some 850 Web gambling sites are based [in Antigua] and an estimated 80% of all gaming URLs on the Web can be traced back to servers on the 108-square-mile island.”); UNITED STATES GENERAL ACCOUNTING OFFICE, REPORT GAO-03-89, INTERNET GAMBLING: AN OVERVIEW OF THE ISSUES 52 (2002), available at <http://www.gao.gov/new.items/d0389.pdf> [hereinafter GAO REPORT] (listing 35 of 88 internet gambling websites as registered in either Antigua or Barbuda, but failing to report the percent of internet gambling taking place at these sites).

47. Indeed the United States even brought a case against the country of Antigua and Barbuda before the WTO in an effort to curtail the proliferation of internet gambling operations on that tiny island nation. The United States lost that suit. See Naomi Rovnick, *Herbies Helps Antigua in WTO Outsourcing Victory*, LAWYER, April 5, 2004, at 10.

48. In 2002, roughly ninety percent of internet transactions used credit cards. Ronald J. Mann, *Regulating Internet Payment Intermediaries*, 82 TEXAS L. REV. 681, 681 (2004).

those technologies have not yet gained any significant base of users, and there is little reason to think that they will gain such a user base in the foreseeable future.⁴⁹ The most common new payment mechanism for internet transactions are the P2P systems,⁵⁰ such as PayPal, which allow individuals who are not merchants to receive payments, but even that market has rapidly become highly concentrated.⁵¹ For Internet actors with a business model that involves the receipt of money, that concentrated and barrier-protected model provides a highly visible “choke point” for regulatory intervention: an internet pharmacy in Canada cannot profitably sell pharmaceuticals to American citizens if it does not accept payment devices that American citizens are likely to use.⁵²

c. Auction Intermediaries.—Our last major type of intermediary is the auction intermediary, which provides the service of matching buyers to sellers, through the mediating device of a website that facilitates sales between remote parties. Although there are other competitors, eBay is the dominant and typical player in this multibillion-dollar industry, and thus not surprisingly the target of most complaints about failure to act to prevent the auction of illegal goods.⁵³

C. Existing (Fault-Based) Liability Schemes

As a general matter, it is likely that the primary malfeasor is the actor that can most efficiently prevent most forms of internet-related misconduct. When an internet worm is released onto the internet, for example, the person who can most easily prevent the harm is the person that wrote the worm and released it onto the internet. For internet gambling to be successful, there must be both a gambler and a gambling website. If either of these individuals is lacking, the gambling will not take place. Thus, if either of these actors can be controlled directly, then the social harm caused by internet gambling can be prevented. This direct approach is the path that the law traditionally has pursued.

But regulation that seeks to prevent misconduct through controlling primary malfeasors is not always effective. These laws are ineffective when individuals are judgment proof or when

49. See RONALD J. MANN & JANE K. WINN, *ELECTRONIC COMMERCE* 576–97 (2d ed. 2005).

50. In this context, P2P stands for “person-to-person.” The term is to be distinguished from the more common use of the same acronym to describe the peer-to-peer filesharing discussed in the context of piracy.

51. See Mann, *supra* note 48, at 683.

52. Recognizing that situation, the OECD at one point even considered using payment intermediaries for collecting taxes on internet commerce. That proposal, however, failed in the face of opposition from those intermediaries. See Arthur Cockfield, *Transforming the Internet into a Taxable Forum: A Case Study in E-Commerce Taxation*, 85 MINN. L. REV. 1171, 1257 (2001).

53. See MANN & WINN, *supra* note 49, at 300-15.

prosecution is not efficient either because of the high volume of transactions or because of the low value of each transaction. Thus, to use the obvious and well-known example, direct regulation of individuals that share copyrighted material on the internet has not, to date, been effective to significantly decrease that type of conduct.⁵⁴ The rise of the internet only exacerbates that problem by making it easier for even solvent malfeasors engaged in high-volume conduct to avoid responsibility either through anonymity or through relocation in a jurisdiction outside the influence of concerned policymakers.

When targeting primary malfeasors is ineffective, policymakers must choose between allowing proscribed conduct harms to continue unchecked⁵⁵ and identifying alternative regulatory strategies. Generalizing broadly, existing formal policy responses have proceeded along two paths, both of which have resulted for the most part in a relatively broad freedom from liability for intermediaries.⁵⁶ First, in a variety of contexts, courts have applied traditional fault-based tort principles to evaluate the conduct of intermediaries. Although there are instances in which relatively egregious conduct has resulted in liability,⁵⁷ many if not most of the cases have absolved intermediaries from responsibility.⁵⁸ Second, in contexts in which courts have held open the prospect that intermediaries might have substantial responsibility for the conduct of primary malfeasors, Congress has stepped in to overrule the cases by granting intermediaries broad exemptions from liability.⁵⁹ Because courts have interpreted those statutes quite broadly,

54. But for some innovative approaches to solving the problem, see WILLIAM W. FISHER III, *PROMISES TO KEEP* (2004); Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement without Restricting Innovation*, 56 *STAN. L. REV.* 1345 (2004).

55. As we discuss below, one realistic possibility of course is that responsible policymakers have settled on a system that declares conduct to be unlawful only because the conduct in fact cannot practicably be proscribed. In such a case, policymakers have no interest in making enforcement more effective. Many would argue that P2P filesharing is (or should be) just such an area.

56. As we emphasize throughout, regulators in a variety of contexts have reached informal agreements with intermediaries in which intermediaries voluntarily agree to cooperate. Our impression is that most of those agreements do not reflect the view of the intermediaries that they could be forced in litigation to provide that cooperation, but rather the view that a failure to cooperate would result in formal legislative regulation: the settlements proceed not in the shadow of existing law, but in the shadow of potential law. That seems to us one reason why, for example, PayPal—hoping to avoid onerous state licensing requirements—seems to have been much more responsive to those efforts than entities like Visa and MasterCard. For discussion of state regulatory treatment of PayPal, see Mann, *supra* note 48.

57. See *A & M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896 (N.D. Cal. 2000).

58. We do not here take a view on the correctness of that doctrine; we simply note it as part of the background that motivates our project. For trenchant criticism, see Landes & Lichtman, *supra* note 28.

59. The most obvious example of this action can be found in the history of the Communications Decency Act. Congress directly responded to the ISP liability found in *Stratton Oakmont, Inc. v. Prodigy Services*, 23 *Media L. Rep.* (BNA) 1794 (N.Y. Sup. Ct. 1995), 1995 WL 323710, by including immunity for ISPs in the CDA, 47 U.S.C. § 230(c)(1) (2004) (exempting ISPs for liability as the “publisher or speaker of any information provided by another information content provider”), which was pending at the time of the case. Similarly, Title II of the Digital Millennium Copyright Act, codified at 17 U.S.C. § 512, settled tension over ISP liability for copyright infringement committed by their subscribers that had been created by the opposite approaches to the issue by courts. Compare *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993) (finding liability), with *Religious Tech. Ctr. v. Netcom, Inc.*, 907 F. Supp. 1361, 1372 (N.D. Cal. 1995) (refusing to find liability).

they have the potential to provide considerable protection for intermediaries, even beyond the context that motivated their enactment.⁶⁰ Although the parallels are not complete, other jurisdictions seem to be taking a similar approach.⁶¹ The paths share not only the reflexive and unreflective fear that recognition of liability for intermediaries might be catastrophic to internet commerce; they also share a myopic focus on the idea that the inherent passivity of internet intermediaries makes it normatively inappropriate to impose responsibility on them for conduct of primary malfeasors. That idea is flawed both in its generalization about the passivity of intermediaries and in its failure to consider the possibility that the intermediaries might be the most effective sources of regulatory enforcement, without regard to their blameworthiness.

The recent litigation involving Perfect 10, Inc. (Perfect 10) is a salient example of the ineffectiveness of tort principles in imposing liability on internet intermediaries.⁶² Perfect 10 owns copyrights in a large number of arguably pornographic⁶³ photographs, which it exploits through a printed periodical and through a website.⁶⁴ Apparently because of the significant

60. *Gentry v. eBay, Inc.*, 121 Cal. Rptr. 2d 703 (Ct. App. 2002) (holding that the Communications Decency Act insulates eBay from claims for facilitating the sale of counterfeit goods); *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1091-92 (C.D. Cal. 2004) (holding that the DMCA shelters payment intermediaries from claims of copyright infringement).

61. With some minor exceptions, other countries have also seen broad liability exemptions for internet intermediaries as the appropriate response to judicial findings of liability. The United Kingdom Parliament took no action after the Queen's Bench in *Godfrey v. Demon Internet Ltd*, QB, [2001] QB 201, held an internet service provider liable as the publisher at common law of defamatory remarks posted by a user to a bulletin board. In the U.S., § 230 of the CDA apparently would prevent such a finding of liability. Similarly, courts in France have held ISPs liable for copyright infringement committed by their subscribers. *See Cons. P. v. Monsieur G.*, TGI Paris, Gaz. Pal. 2000, no. 21, at 42-43 (holding an ISP liable for copyright infringement for hosting what was clearly an infringing website).

In 2000, however, the European Parliament passed Directive 2000/31/EC, available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf, which in many ways mimics the DMCA in providing immunity to ISPs when they are acting merely as conduits for the transfer of copyrighted materials and when copyright infringement is due to transient storage. *Id.* Art. 12, 13. Further, the Directive forbids member states from imposing general duties to monitor on ISPs. *Id.* Art. 15. This Directive is thus in opposition to the British and French approaches and requires those countries to respond statutorily in much the same fashion as Congress responded to *Stratton Oakmont* and *Religious Technology Centers*. Of course courts are always free to interpret the Directive or national legislation under the Directive as not applying to the case at hand. *See, e.g.*, *Perathoner v. Pomier*, TGI Paris, May 23, 2001 (interpreting away the directive and national legislation in an ISP liability case).

Canada has passed legislation giving ISPs immunity similar to the DMCA. *See Copyright Act*, R.S.C., ch. C-42, §2.4(1)(b) (stating "a person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate that work or other subject-matter to the public"). The Canadian Supreme Court interpreted this provision of the Copyright Act to exempt an ISP from liability when it acted merely as a "conduit." *Soc'y of Composers, Authors and Music Publishers of Can. v. Canadian Assoc. of Internet Providers*, [2004] S.C.C. 45, 240 D.L.R. (4th) 193, ¶92. The court in that case also interpreted the statute to require something akin to the takedown provision of the DMCA. *See id.* at ¶110.

62. Our account draws not only on the various published opinions in the litigation, but also in pleadings we have obtained from PACER.

63. We use the term "pornography" loosely to refer to material marketed with claims of a generally prurient appeal. We make no effort to distinguish here between material that is or is not protected by the First Amendment or between content that is or is not lawful under applicable state and federal laws. The discussion in Part IV below is limited to child pornography so as to avoid the difficult line-drawing questions inherent in regulation of adult-related businesses more broadly. *See Ashcroft v. ACLU*, 535 U.S. 564 (2002) (consideration of those problems by a divided Court).

64. *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 167 F. Supp. 2d 1114, 1117-18 (C.D. Cal. 2001) [hereinafter *CyberNet I*].

commercial value of those photographs, they regularly have appeared on a substantial number of websites without Perfect 10's consent, in relatively flagrant violation of Perfect 10's rights under copyright law.⁶⁵ The open contempt for intellectual property rights by the primary defendants in these cases is evidenced by the common practice of taking Perfect 10 photographs of relatively unknown models and attaching to them a photograph of a widely recognized celebrity (Britney Spears being the most prominent).⁶⁶

In an effort to protect its intellectual property, Perfect 10 instituted several separate causes of action. The most directly responsible defendant probably was Cybernet, a company that operated a system that verified the age of customers by using credit card accounts.⁶⁷ Among its various activities, Cybernet operated a consortium of privately run internet websites that provided pornographic material.⁶⁸ To facilitate this network, Cybernet charged customers a monthly fee and provided those customers with a password that could be used to access over 300,000 (not a typo!) privately run pornographic websites.⁶⁹ Perfect 10 claimed that Cybernet was liable for direct, contributory, and vicarious copyright infringement, direct and contributory trademark infringement, and unfair competition.⁷⁰ Although Perfect 10 lost on many of those claims, the district court concluded that CyberNet's participation in the copyright infringement on the sites in its network was sufficiently direct to justify preliminary relief on claims for contributory and vicarious copyright infringement and aiding and abetting unfair competition.⁷¹

Of more interest to our project, however, are Perfect 10's actions against Visa, MasterCard, and Google.⁷² Perfect 10 claimed, for example that Visa and other companies that facilitated the credit card transactions were liable for contributory copyright infringement because they made it possible for Cybernet websites to operate profitably.⁷³ Among other things, it was clear that Visa

65. Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002) [hereinafter *CyberNet II*].

66. *CyberNet I*, 167 F. Supp. 2d at 1118, 1125.

67. *CyberNet II*, 213 F. Supp. 2d at 1158. The system generally rests on the not entirely accurate assumption that those who hold credit card accounts are not minors.

68. *Id.* at 1158–59.

69. *Id.*

70. *Id.* at 1165–89.

71. *Id.* at 1168–69, 1171, 1174, 1184, 1188–89.

72. Perfect 10 also instituted litigation against a number of less prominent intermediaries, including a group of related entities that included ISPs, payment intermediaries, and search engine providers. For the most part, the analysis in that litigation turns on details of copyright law that are not interesting for our purposes. For example, the court dismissed some of Perfect 10's claims based on Perfect 10's failure to send notices that complied with the DMCA, dismissed others for failure to show any defects in the entity's policy for terminating repeat infringers, and allowed some actions to proceed based on the failure of the defendant to submit any such policy. Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1086–1103 (C.D. Cal. 2004).

73. Perfect 10, Inc. v. Visa Int'l Servs. Ass'n, 2004 WL 1773349, at *1-*2 (N.D. Cal. Aug. 5, 2004).

and MasterCard were aware of the dubious nature of Cybernet's activities because high chargeback rates on Cybernet transactions had motivated both networks to place Cybernet in a category for high-risk merchants.⁷⁴ Although the opinions do not make it clear, it is plain from the pleadings that one of the consequences of placing CyberNet in that category is that Visa and MasterCard charged higher fees to CyberNet than they otherwise would have charged.

In what seems to us a perfectly plausible application of existing law, the court had little difficulty in dismissing the action against Visa and MasterCard.⁷⁵ The court relied heavily on the content-neutrality of Visa and MasterCard services:

Defendants provide content-neutral services. Defendants do not promote the websites that use their services. Nor do Defendants have content-specific regulations with which merchants must comply before using Defendants services, as Cybernet did. Defendants do not hold out certain merchants as being providers of a particular quality of product. Defendants are concerned solely with financial aspects of the websites, not their content.⁷⁶

We would analyze these cases quite differently. The approach of the courts exonerates Visa and condemns Cybernet based on the (apparently accurate) conclusion that Visa's level of participation in the misconduct was considerably less than Cybernet's. In terms of equity, Visa has clean hands and Cybernet does not. That might make sense in a legal system designed to force bad actors to provide redress to injured parties. The better question, however—albeit one not readily susceptible of judicial analysis—is whether either Visa or Cybernet is the party best situated to stop the copyright violations in question. On that point, Visa probably is much better situated, because of the real-world likelihood that none of the sites that fosters the infringement could survive as a profitable commercial enterprise if it could not accept payments from Visa.⁷⁷ This is not to say that Cybernet should be exempt from traditional copyright liability if its participation in the conduct is sufficiently direct (which it seems to be). It is to say, however, that a separate form of liability for Visa and MasterCard should be considered—one that rests not on

74. *Id.* at *2.

75. The action against Google has not yet been resolved. Google now faces a similar action brought by the French news agency Agence France Presse. See Lisa Baertlein, *Agence France Presse Sues over Google News*, REUTERS, Mar. 18, 2005, available at <http://www.reuters.com/newsArticle.jhtml?type=internetNews&storyID=7949422> (last visited Mar. 25, 2005).

76. *Perfect 10, Inc. v. Visa Int'l Servs. Ass'n*, 2004 WL 1773349, at *3 (N.D. Cal. Aug. 5, 2004).

77. We assume that any rule would apply equally to MasterCard, to Visa, and to the leading payment intermediaries, so that a ruling in favor of Perfect 10 would prevent the site from accepting payments from either of the dominant providers. To the extent the court erred, it is in its assumption that a ruling against the payment intermediaries would have no effect on CyberNet's business. *Id.* at *4. We think it most unlikely CyberNet could survive as a profitmaking entity without access to one of a small number of dominant payment intermediaries.

the degree of passivity but rather on the structural relation between the payment providers and the challenged conduct.

III. Liability Without Fault: Internet Intermediaries as Gatekeepers

A. *The Basic Premise*

The basic premise of this Essay is that the response described above is a wrong turn. Fundamentally, we argue, it is inadequate to respond to internet-related misconduct with rules for intermediaries that turn so pervasively on normative and fault-related notions of responsibility and participation. The touchstone that we suggest—searching for the least-cost avoider—is not a new one. Nor is it a new idea that in some cases misconduct can be sanctioned most effectively through the indirect imposition of responsibility on intermediaries. That idea is prominently associated with a pair of papers on the subject of “gatekeeper” liability written in the early 1980’s by Reinier Kraakman.⁷⁸ To understand its importance, it is necessary to understand both the distinctive nature of the gatekeeper regime and the reasons it is so well-suited to the internet.

1. *The Nature of Gatekeeper Liability.*—The first point is the simplest one, already emphasized above: the imposition of liability under the gatekeeper rationale should have nothing to do with a normative assessment of the level of responsibility, participation, or support of the intermediary. Rather, it should turn entirely on the balance between the social costs of the misconduct and the effectiveness with which the intermediary can sanction the misconduct (more on that calculus below). That is not to say that it is inappropriate to impose liability in cases in which the intermediary *is* directly involved in the misconduct. For example, in *Napster*, it seems not an unfair assessment of the facts to conclude, as the Ninth Circuit did, that Napster was so involved in unlawful P2P filesharing⁷⁹ as to make it appropriate to sanction Napster for that misconduct. The gatekeeper inquiry, however, would turn on the question whether Napster could serve as a reliable tool for preventing unlawful filesharing. As we discuss below, the fact that no actions by Napster could possibly have stopped unlawful filesharing suggests that imposition of gatekeeper responsibility on Napster would have been ineffective.⁸⁰

78. Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53 (1986) [hereinafter Kraakman, *Gatekeepers*]; Reinier H. Kraakman, *Corporate Liability Strategies and the Costs of Legal Controls*, 93 YALE L.J. 857 (1984) [hereinafter Kraakman, *Corporate Liability Strategies*].

79. That assumes of course something that is not yet entirely clear: that there is very little personal trading of music that constitutes fair use under Copyright Act § 107.

80. As that discussion emphasizes, we do not suggest that Napster could not have stopped filesharing on *its* network. On the contrary, it seems plain that Napster readily could have eliminated the great majority of unlawful filesharing on its network. Our point is the more systemic one that even the complete eradication of Napster (and Grokster) will do little to

To put the point affirmatively, the key question for determining the propriety of intermediary liability is how plausible it is to think that the intermediary could detect the misconduct and prevent it.⁸¹ Specifically, because the analysis premises the imposition of responsibility on a determination that the intermediary is the least-cost avoider of the misconduct in question, a proper determination requires not only that the gatekeepers be *able* to detect offenses, but they also be able to detect and prevent them *economically*. Thus, for example, if the sole effect of the regulation of a particular intermediary will be to motivate illicit actors to shift constantly to ever more elusive intermediaries—with no effect on the underlying misconduct—then the costs of the regulation are likely to be a total loss. This suggests to us that one of the central factors in assessing the best regulatory strategy must be the market structure of the various intermediaries: intermediaries with market power that prevents illicit actors from moving to substitutes are much better targets than those for whom there are ready substitutes. Thus, continuing with the example above, focusing attention and regulatory resources on entities like Napster, Grokster, and their progeny makes sense only if it is plausible to believe that their eradication would stop piracy. Conversely, attention to entities like eBay or the dominant payment intermediaries is particularly effective in contexts where the illicit conduct depends directly on access to the facilities of those intermediaries.

The point here is not to make a definitive assessment of the potential technological responses, which would be both beyond our capabilities and short-lived in its accuracy in any event.⁸² The point is simply to emphasize that a strategy making use of intermediaries makes sense only in contexts where the inevitable costs can be balanced against benefits in real reductions—rather than relocations—of misconduct.⁸³

slow unlawful filesharing, which—in the absence of a significant escalation in the ability of content providers to intervene in the architecture of the internet—will continue to proceed on ever more elusive networks. For a cautionary note on the risks of such intervention, see Zittrain, *supra* note 26.

81. Kraakman, *Gatekeepers*, *supra* note 78, at 54; Kraakman, *Corporate Liability Strategies*, *supra* note 78, at 890–94.

82. For example, it is not at all far-fetched to think that ISPs—or even consumer’s own computers—soon could be put in a position to monitor the particular applications being used by their customers. Zittrain, *supra* note 26. If this sounds implausible, consider the conventional wisdom that manufacturers of photocopiers cannot build their machines to prevent private copyright infringement. *E.g.* Landes & Lichtman, *supra* note 28, at 409 (“[A]lthough firms that produce photocopiers might not be able to discourage piracy directly, they can easily build into their prices a small fee that could in turn be used to compensate injured copyright holders.”) But as the relentless march forward of technology continues, this conventional wisdom is brought into doubt when one learns about new technologies being implemented such as the one the U.S. Treasury is using to fight currency counterfeiting. The technology gives digital scanners the ability to recognize currency when it is scanned. The scanners then override the scan and direct users to a website that contains information about the use of currency images. Ted Bridis, *Low-Quality Images of New \$50 Bill Offered; Making Digital Copies Is Getting More Difficult*, TELEGRAPH HERALD (Dubuque, IA), Oct. 10, 2004, at B13.

83. See Doron Teichman, *The Market for Criminal Justice: Federalism, Crime Control and Jurisdiction Competition* (unpublished 2005 manuscript) (on file with author).

2. *Gatekeeper Liability and the Internet.*—The second point is an overtly exceptionalist argument that gatekeeper liability is systematically more likely to be effective in the modern internet environment than it has been in traditional offline environments.⁸⁴ This is true for three separate reasons. First, as should be clear from the discussion of the structure of the internet in Part I, it often will be the case that a particular type of misconduct on the internet generally will proceed through a readily identifiable intermediary or class of intermediaries, and that it will not at reasonable cost be practicable for those who wish to engage in misconduct to avoid such an intermediary: the customer who wishes to purchase contraband on the internet is quite likely to interact with a site that describes or provides the contraband and to use some form of payment intermediary to pay for the contraband. This is of course a substantial change from offline reality, in which the seller of contraband need not establish a freely accessible place of business and in which wholly untraceable cash payments are easy.

Second, advances in information technology make it increasingly cost-effective for intermediaries to monitor more closely the activities of those that use their networks. As it becomes cheaper to monitor activity more closely, it ineluctably becomes *relatively*⁸⁵ more desirable to rely on such monitoring as the least expensive way to eradicate undesirable activity.⁸⁶

Third, the relative anonymity that the internet fosters makes remedies against primary malfeasors much less effective than they are in a brick and mortar context. Thus, for example, it is much easier to obtain a relatively anonymous email account (from a provider such as Google) for use in connection with illicit conduct than it is to obtain a post-office box in the offline world. This is not to say that anonymity is impossible in the offline world or that it is perfect in the online world; it is simply to say that it is much easier to engage in relatively anonymous conduct online than it ever has been offline. But with the introduction of intermediaries in targeting certain activities, this anonymity decreases significantly. The networks provided by the intermediaries, whether communication networks in the case of ISPs, payment systems in the case of payment intermediaries, or auction systems in the case of auction intermediaries, require that users of those networks be identifiable to varying extents. ISPs provide service to an

84. Joel Reidenberg notes the possibility that intermediary enforcement might be “more efficient” if illegal activities are “channeled through gateway points.” Reidenberg, *supra* note 22. He does not, however, focus as we do here on the systematic reasons why that might be so.

85. We suggest only that it becomes *relatively* more desirable. As we emphasize throughout, the costs of monitoring in many cases might make large-scale monitoring unjustified except in cases of serious misconduct.

86. This point of course can be overstated. Just as technology in the last few years seems to have made monitoring easier, it is entirely possible that technology in the near future will make it easier for wrongdoers to avoid monitoring. As discussed below, it is our impression that this has been happening in the filesharing area, where advances in P2P technology have made it difficult to locate and identify resourceful filesharers and those who assist them. It is not clear, however, whether this always will be so. See Zittrain, *supra* note 26.

identifiable account holder. The electronic payment systems currently in widespread use require transfers to identifiable accounts. And auction intermediaries obtain personal information in order to facilitate the smooth operation of auctions and to ensure payment. Thus, when these types of intermediaries are engaged in the battle against an activity, the information they collect in order to provide their services automatically and necessarily decreases the anonymity of the transaction.

B. Variations on the Theme

Traditional discussions of gatekeeper and intermediary liability have proceeded on the implicit assumption that a standard damage remedy will be used to induce the intermediary to curtail misconduct by the primary malfeasors that are under the control of the intermediary. Thus, one of the principal topics in the literature has been the question whether the liability of the gatekeeper should be strict or based on negligence or fault.⁸⁷ From our perspective, however, a more contextual assessment of the multifarious types of internet intermediaries suggests that a wider array of policy options should be considered. For present purposes, it is enough to describe three types of remedies: a traditional tort remedy for damages, a takedown regime (the DMCA being the leading example), and a “hot-list” regime (common in bank regulation).

A traditional tort remedy imposes the greatest risk on the intermediary, because, depending on the details, it leaves the intermediary exposed to damages if the intermediary fails to take adequate steps to detect and control misconduct.⁸⁸ If the risk of liability is not readily predictable or cabined, that remedy is most likely to have adverse collateral effects (such as overdeterrence).⁸⁹ That problem is particularly serious when that remedy applies to misconduct that is not entirely avoidable by the intermediary. Consider, for example, a regime in which an ISP is responsible for copyright infringement for all unlawful filesharing in which its customers engage. If monitoring technology makes it feasible for the ISP to detect some—but not all—of the conduct in question, then we might expect that a remedy holding the ISP strictly liable for the misconduct will have a considerable adverse effect on *all* users—either through restrictions on service or through an increase in price. Conversely, because it applies only *ex post*, a damages remedy would have the undetering aspect that it would have no effect on the conduct of

87. See, e.g., Assaf Hamdani, *Gatekeeper Liability*, 77 S. CAL. L. REV. 53 (2003).

88. This problem of course could be mitigated if the remedy were a statutory fine in a fixed amount. In that case, the key question of course would be how to set the fine so as to provide the appropriate incentive.

89. Here, for example, it is common for cyberlaw scholars to worry that the imposition of any liability on intermediaries for the action of their customers will lead to the prohibition of anonymous postings, which will have adverse effects on internet polity.

financially irresponsible intermediaries. The schemes we discuss below—with more objective *ex ante* requirements—would be more effective in pinpointing irresponsible intermediaries and removing their ability to facilitate misconduct.

The second potential remedy is a takedown scheme. The paradigmatic example, the provisions of the DMCA codified in Section 512 of the Copyright Act,⁹⁰ generally obligates covered intermediaries to remove allegedly illicit conduct promptly upon receipt of an adequate notice of the misconduct.⁹¹ Although this scheme does impose obligations on the intermediaries, it imposes a relatively small risk of liability, because it generally carries with it an implicit exemption from monetary relief so long as the intermediary complies with appropriate takedown notices.⁹² Thus, this response is less costly, and can be justified as a response to a problem with lower social costs than the problems that would justify a damages remedy.

At the same time, this response is less effective, because it does not enlist the aid of the intermediary in identifying and removing illicit material. The dispute between Tiffany and eBay illustrates the problem.⁹³ Let us suppose, as seems likely to be the case, that eBay is more than willing to remove from its auction site any postings for materials that Tiffany can identify to eBay as falsely claiming to be Tiffany trademarked products. Yet, eBay still might sell millions of dollars of counterfeit Tiffany products each year, solely because of the difficulty Tiffany would face in identifying each counterfeit product sufficiently rapidly to forestall a successful auction. Tiffany plausibly might think that eBay could identify those auctions more effectively than Tiffany and wish that eBay were obligated to do so. A takedown remedy, rather than a damage remedy, would provide little help to Tiffany in that circumstance.

The final response is a “hot list” scheme. This type of scheme is common in the financial industry. Generally, in this type of scheme a reliable actor (such as the government) identifies a list of illicit actors. Thus, most commonly, banks have for years been prevented from wiring money to any entity on the federal government’s list of entities that support terrorist activity.⁹⁴

90. 17 U.S.C. §512(c) (2004)

91. Such a system of course could be designed more or less effectively. For example, it might be that the DMCA imposes excessive costs by giving intermediaries an incentive to remove material upon the receipt of ill-founded notices and by providing unduly burdensome avenues of review to the party whose information is taken down.

92. There remains the possibility, not yet settled in the courts, that an intermediary could have traditional liability for direct participation in the initial posting even if the intermediary complied with a takedown notice after the fact. *See CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544 (4th Cir. 2004).

93. *See generally Psst, Wanna Buy a Cheap Bracelet?*, *ECONOMIST*, July 3, 2004, at 13 (describing the controversy between Tiffany & Co. and eBay and concluding that liability for eBay is wrong because of the immense difficulty of monitoring auctions and verifying whether items offered for auction are genuine).

94. In response to the September 11, 2001 terrorist attacks, President Bush made it illegal, by executive order, to transfer property to certain persons listed initially by the Executive Order and subsequently designated by the Secretary of State. Executive Order 13224, Blocking Property and Prohibiting Transactions with Person Who Commit, Threaten to Commit, or

This scheme is likely to provide the most predictable exposure to intermediaries, because their obligations are purely ministerial. Indeed, with advances in information technology that presumably would allow such lists to be examined automatically,⁹⁵ violations by the intermediaries might be quite rare. Of course, this scheme goes even further than the takedown scheme to shift the burden of monitoring away from the intermediary. Here, the government must expend sufficient resources to identify the illicit actors even before the illicit transactions begin.⁹⁶ Thus, this response will be useful only in situations in which the illicit transactions are likely to have a readily identifiable and relatively stable location.

We provide of course only a simple list of options. It is easy to imagine responses that combine features from the various options. Most obviously, the framework above does not specify what the remedy would be for failure to comply with a take-down or hot-list requirement. The remedy for such a failure itself could be calibrated to extend only to a loss of immunity (the result under the existing DMCA regime), or could extend more broadly to secondary liability for the unlawful activity, or perhaps to some intermediate sanction (such as a fine in an amount less than the fine that would be imposed for the unlawful illicit activity).

C. *A Framework for Analysis*

The foregoing subparts doubtless will strike some as evincing undue optimism about the value of imposing liability on intermediaries, as well as a blithe lack of concern about the costs that liability will have on the intermediaries and on those that depend on the services that intermediaries provide. That is not, however, because we are unaware of or unconcerned about those costs. Rather, it is because it is necessary to describe the structure and premises of the proposed liability before we can describe how policymakers should use the tool. Nor should the discussion be taken as directly critical of the efforts of judges working under existing law. It should be plain that the liability schemes that we envision are not the type of thing readily adopted through the development of the common law. Our framework is intended to provide

Support Terrorism (Sept. 23, 2001). Today, the Office of Foreign Asset Control, part of the Department of the Treasury, maintains a list of designated foreign nationals to or from whom banks are forbidden to facilitate transactions. For more on these regulations, see OFFICE OF FOREIGN ASSET CONTROL, FOREIGN ASSET CONTROL REGULATIONS FOR THE FINANCIAL COMMUNITY (2005), available at <http://www.treas.gov/offices/enforcement/ofac/regulations/t11facbk.pdf>.

95. Lists of designated persons are available for download in a variety of electronic forms to increase the ease with which financial intermediaries can integrate required blocking into their existing systems. See Office of Foreign Asset Control, SDN and Blocked Persons Data Formats, at <http://www.treas.gov/offices/enforcement/ofac/sdn/data.shtml> (last visited Jan. 15, 2005).

96. The text assumes that regulators will not delegate to private entities the ability to designate entities to be placed on hot lists, and that regulatory decisions on that point will be made under procedures that provide reasonable notice and opportunity for review. Systems that did not provide those safeguards of course would be more costly and thus less justifiable.

fodder for legislators and regulators, not for judges.⁹⁷ Thus, we hope that our analysis can lead to well-specified statutory schemes or regulatory initiatives. Among other things, a general directive to courts to implement intermediary liability easily could shade into judicial doctrines that would obligate all actors to stop all misconduct whenever they can. As Judge Posner recently explained, such an unbounded principle would be unduly disruptive.⁹⁸ Our hope, in contrast, is that the state regulators that currently are searching for tools to respond to internet-related conduct that they find offensive, will consult the framework that we articulate so that the informal responses that they seek—and, increasingly, obtain—will reflect an appropriate sensitivity to the costs their remedies impose.

Furthermore, we express no views as to the social benefits to be gained from eradicating *any* of the various forms of misconduct discussed in the next Part of this Essay. From our perspective, that is a judgment call to be made by the relevant policymaker: we express no opinion here, for example, on the relative social benefits to be obtained from limiting the sale of counterfeit goods, limiting sharing of copyrighted music, and limiting the dissemination of child pornography. In each case, those benefits, whatever they might be, must be weighed against the costs of imposing intermediary liability. As the discussion above emphasizes, the relevant benefits are the value of eradicating the misconduct that the particular liability scheme in fact will eradicate.

At the same time, the costs of any of these regimes are likely to be substantial.⁹⁹ The existing literature focuses on two general categories of costs, which seem to us illustrative. It is well recognized that the imposition of liability on intermediaries will affect the services and prices they present to their customers.¹⁰⁰ If regulation increases costs substantially, some customers will stop using the gatekeeper's service, those that derive net benefits from the service that are less than the newly imposed costs. In some cases, and especially as the cost of liability to the gatekeepers increases significantly, the problem may spiral out of control, so that the only customers to remain will be those who are using the gatekeepers' services in highly rewarding

97. For analysis criticizing the doctrine judges have developed under the existing statutory scheme for piracy, see Landes & Lichtman, *supra* note 28 (arguing that broad ISP exemptions are inconsistent with traditional rules of tort liability).

98. *Cuylar v. United States*, 362 F.3d 949, 955–56 (2004).

99. For a thorough discussion, see Hamdani, *supra* note 87, at 63–82.

100. See Kraakman, *Gatekeepers*, *supra* note 78, at 77, 93–94; Kraakman, *Corporate Liability Strategies*, *supra* note 78, at 892 (“[F]irms will . . . pay for the risk of additional liability in the familiar ways. If outside gatekeepers cannot shift their liability risks, they will charge high risk premiums.”).

ways.¹⁰¹ In situations where the remaining users are predominantly those committing the targeted acts, the ultimate effects of the regulation are likely to be counterproductive.

Another problem is that gatekeeper liability might upset the market balance for the services provided by gatekeepers. Specifically, there always is the risk that imposing additional burdens on intermediaries can chill the provision of valuable goods and services. That will be especially problematic in cases in which there is considerable risk of chilling legal conduct that is adjacent to the targeted conduct. As we discuss below, that might tend to make the use of intermediaries less plausible in file-sharing contexts (where it is quite difficult to be sure any particular act of file-sharing is illegal) and much more plausible in the gambling context (where it is plausible in many cases that substantially all traffic to a particular site involves illegal conduct). Requiring intermediaries to make those kinds of subjective decisions imposes costs not only on the intermediaries (that must make those decisions), but also on the underlying actors whose conduct might be filtered incorrectly. To the extent the regulation affects conduct that has positive social value¹⁰²—as it is likely to do in at least some of our contexts—the direct and indirect effects on that conduct must be counted as costs of any regulatory initiative. Thus, we emphasize that in any particular case, the costs of any particular regime described in this essay might exceed the benefits that could accrue from implementing the regime, and in such a case we would not support a new regime.

But the premise of any regulatory state is that society successfully can impose burdens on actors that will provide substantial social benefits while not overdetering those individuals from providing their services. We see this when the local, state, and federal governments impose tax burdens on private actors. Taxes are an additional burden on business, but in situations where the taxes are well-designed, society can benefit both through the provision by the business of taxable goods and services and also by the use to which the government puts the tax revenues.

* * *

In sum, we pose a traditional cost-benefit calculation, in which the policymaker should assess the costs, broadly defined, of the particular scheme of intermediary liability. If those costs exceed the benefits, then the particular form of intermediary liability might be appropriate. If they do not, then the new liability is not appropriate.

101. This is the problem of “unraveling” markets, discussed in detail by Hamdani. *See* Hamdani, *supra* note *supra* note 87, at 72–73.

102. Assaf Hamdani emphasizes the point that this problem will be particularly serious because intermediaries will fully internalize the sanctions they will face for failure to filter with sufficient vigor, but will not internalize the social costs of excessive filtering. Hamdani, *supra* note 29.

IV. Applications to Specific Types of Conduct

The nuance that is necessary to do a responsible job of enlisting intermediaries in the quest to cabin misconduct on the internet can best be seen through concrete examples. For our purposes, two distinct categories of misconduct are useful: wrongful dissemination of content and breaches of security. The first category broadly includes the use of the internet to provide material that violates applicable law. The examples on which we focus here are advertising the sale of contraband or counterfeit goods, internet gambling, child pornography, and sharing copyrighted files. The second category includes breaches of security—viruses, hacking, spam, and the like—which threaten the integrity of the computer systems that have become so essential to our modern economy.

A. *Dissemination of Content*

The basic problem with regulating content in an internet era is that content can reside on any computer in the world that can be connected to the internet. Thus, regulations that prohibit the dissemination of particular content often cannot reach those that make content available in places where it is unlawful. A policymaker could respond to that situation in any number of ways: by accepting a status quo in which laws on the books tacitly are flouted by widespread internet conduct, by formalizing the futility of regulation by abandoning the regulations entirely, or by adopting a new system of regulation that is more effective than targeting primary malfeasors. Our analysis in this subpart does not advocate any one of these options for any of the particular types of misconduct that we address. Rather, our aim is the more modest one: To illustrate the features of particular situations that might make a specific form of intermediary liability a more or less useful device for limiting misconduct.

1. *Trafficking in Contraband and Counterfeit Products.*—The simplest problem is the problem of contraband and counterfeit products. To use the prominent example discussed above,¹⁰³ Tiffany & Co. has been engaged in a long-running dispute with eBay about the sale on eBay of counterfeit Tiffany & Co. merchandise. There are, however, other obvious problems that have drawn attention from regulators: the sale of pharmaceuticals to United States residents that have not been approved for use by the FDA (principally from Canadian retailers),¹⁰⁴ the sale of cigarettes in violation of local and federal tax laws¹⁰⁵ are notable.

103. See *supra* note 93 and accompanying text.

104. See *supra* note 18.

105. See *supra* note 17.

In some ways, these situations are much more tractable than the situations discussed in the sections that follow, because much of the conduct is likely to involve the shipment of products to addresses located in jurisdictions in which the sale of the product is plainly illegal.¹⁰⁶ Thus, for example, it is easy to see that Massachusetts should be able to proscribe the shipment of firearms to an address physically located in Massachusetts.¹⁰⁷ A rule limited to such shipments would be both underinclusive (it would not bar shipments to addresses just outside Massachusetts even if the products ultimately would be distributed in Massachusetts) and perhaps overinclusive (some shipments to Massachusetts addresses might be intended for use outside the state). Yet, a practical scheme for prohibiting such shipments would go a long way (particularly in states larger than Massachusetts) to prohibiting the targeted conduct and impose relatively little cost on innocent third parties: it is not too much to ask, we think, that persons that want to buy guns that are illegal in Massachusetts should come up with a mailing address outside the borders of the state. Even in cases of nonuniform regulation (like firearms or wine), the analogy of the Streamlined Sales Tax Project¹⁰⁸ suggests that it should be easy enough under current technology for responsible retailers to refrain from shipping contraband into prohibited jurisdictions.

In some cases, however, direct enforcement against a retailer will be ineffective. For example, in some cases a jurisdiction might face a large number of small, relatively irresponsible retailers, so that direct enforcement would be prohibitively expensive in practice. Two more general examples are cases in which the retailer takes advantage of the relative anonymity afforded by an auction site like eBay or cases in which the retailer is located outside the United States, in a jurisdiction that will not cooperate with the applicable state regulators. Even in those cases, it is important that the business model for the primary malfeasors generally involves a retail sale of the product in return for monetary compensation. Among other things, this generally involves the existence of a website at which the nature and availability of the product is evident to all (at least in an era of effective search engines). This has several ramifications for the design of a policy response. Most obviously, it means that intermediaries often would be able to detect and control the conduct. We discuss here auction intermediaries and payment intermediaries, which seem to be the simplest and most common possibilities.

106. The conduct that does not involve physical shipments is harder to deal with both because of the threshold question whether the illegal conduct in fact occurs in the targeted jurisdiction—how exactly do we decide where online gambling occurs?—and because of the consequent difficulty in designing practical ways for intermediaries to identify illegal conduct that is adequately related to the regulating jurisdiction.

107. *See supra* note 24.

108. *See* www.streamlinedsalestax.org. For discussion, see Cockfield, *supra* note 10, at 386-88, 397-98.

a. Targeting Auction Intermediaries.—Auction intermediaries are particularly relevant for the problem of counterfeit trademarked goods—the other contraband problems mentioned above tend to involve offshore suppliers of products that violate local regulatory schemes. eBay, in contrast, is an entity with a major domestic presence that owns facilities through which a substantial amount of counterfeit goods are sold. In that context, it seems clear that eBay could detect and prohibit many of the sales of counterfeit Tiffany & Co. products at its site.¹⁰⁹ What we are really talking about, then, is the question whether the burden should be on Tiffany & Co. to locate counterfeit products and bring them to eBay’s attention (as it would be under a DMCA take-down regime) or whether the burden is on eBay in the first instance to locate those products and remove them.

Viewed from the perspective set forth above, the relevant policy considerations are easy to discern. On the one hand, it is at least plausible to think that eBay is better-placed to identify those products in the first instance. Surely eBay is more adept at searching and monitoring its marketplace than Tiffany & Co.; at the same time, eBay probably is not as effective as Tiffany & Co. is at the task of distinguishing bona fide Tiffany products from counterfeits.¹¹⁰ The net benefit of shifting that task to eBay from Tiffany—the combination of cost savings and any increased detection of misconduct—is the potential benefit of intermediary liability in this context. The magnitude of that benefit is difficult to quantify, because it depends in part on the social value of the increased detection of that misconduct. The costs, on the other hand, are the burdens that shifting that task to eBay would impose on all users. Among other things, that burden is likely to diminish the functionality of eBay’s site even for innocent users by setting up additional steps that will slow the availability of their postings.

If the social benefits of removing the contraband or counterfeit products were high enough, it might be plausible to impose a damages regime—under which eBay and other intermediaries would be strictly liable for this conduct. Given the difficulties eBay would face in complying with a mandate to remove *all* counterfeit products, it might be more plausible, however, to adopt a takedown regime of some kind—perhaps a regime under which eBay would be obligated to

109. Tiffany & Co. complains of sales of products that are advertised falsely as Tiffany & Co. products and also of products that appear to bear a counterfeit Tiffany & Co. mark but are not advertised as such. *See Psst, Wanna Buy a Cheap Bracelet?*, *supra* note 93. The first category apparently could be detected by textual searches of advertising copy. The second category would be more difficult to detect without a search engine that could search visually for a particular mark. The development of such a search engine—certainly plausible under existing technology—well might shift the appropriate locus of responsibility.

110. Indeed, it may be that we err in assuming that monitoring is the lowest-cost method of eradicating contraband from eBay. We can imagine, for example, circumstances in which it might impose a lower net burden on eBay’s business for eBay to require bonds from its customers to ensure their compliance with applicable restrictions on contraband. Given the small size and presumptive illiquidity of many eBay merchants, we doubt that would be the optimal response. Our main point, however, is that eBay plainly is better situated to assess the relative costs of different remedies than Tiffany.

remove all counterfeit products for the owners of famous marks¹¹¹ that made a suitable request.¹¹² Similarly, particularly if the costs of compliance were sufficiently great that they might alter the pricing of eBay's services to all customers, it might make sense to permit eBay to impose those costs on the content owner: permitting eBay to charge content owners, Tiffany & Co., for example, a "reasonable fee" for complying with a statutory mandate to remove counterfeit products.¹¹³

b. Targeting Payment Intermediaries.—To the extent that contraband and counterfeit products tend to be sold from a stable site,¹¹⁴ the payment intermediary also can serve a useful role—perhaps a broader role given the importance of payment to the offshore venues from which contraband goods are shipped into the United States. As discussed above, roughly 90% of modern internet retail transactions use a credit or debit card as a payment vehicle.¹¹⁵ Furthermore, although precise data is difficult to locate, it is plain that the lion's share of those transactions in this country make payment either through the Visa network or through the MasterCard network, and that all of those transactions pass through a small handful of networks. What that means, in turn, is that a remedy that prevented any of that small number of networks

111. This is not as vague as it sounds, because it is a term of art defined in Section 43 of the Lanham Act, 15 U.S.C. § 1125.

112. This would differ from the existing DMCA in that the notice from the content owner would not identify specific products to be removed, but rather specific marks to be examined.

113. This would more directly link the cost of eliminating the harms to the entity that benefits from its elimination. Whether this should be done depends on one's view of the baseline: is Tiffany & Co. entitled to a world free of trademark dilution resulting from eBay's business, or is eBay entitled to a world in which it can freely connect buyers and sellers? To put it in economic terms, why can't we view the risk to Tiffany as an externality created by eBay's new business, which eBay should be forced to internalize to ensure that its business in fact increases net social value. From that perspective, one likely view is that it is appropriate to require the trademark owner to pay the reasonable costs of compliance to ensure that the private value of the mark exceeds the transaction costs of the takedown. In a perfect world of course the baseline would be irrelevant because the trademark owner would negotiate to purchase a takedown from eBay if that were an efficient outcome. Here, there is some reason to think that might happen, where transaction costs between two large companies are low when compared to the value of the rights being negotiated. Of course, it would be naïve to think that the selection of a particular baseline as a legal rule would be irrelevant. As Bebchuk explains, the selection of a particular liability baseline is likely in many contexts to have significant long-run effects on the allocation of investments related to the activity in question. See Lucian Arye Bebchuk, *Property Rules and Liability Rules: The Ex Ante View of the Cathedral*, 100 MICH. L. REV. 601 (2001). The problem is quite similar to the problem of default rules in contracting, where the modern literature recognizes that the choice of the default rule has important implications for the ultimate allocation of resources. Ronald J. Mann, *Contracts—Only with Consent*, 152 U. PA. L. REV. 1873, 1896–1901 (2004). This problem is much less relevant to the sections of our analysis (such as child pornography and gambling), where the dispute over liability involve the government and a commercial party rather than two commercial parties. In those situations, one can hardly imagine, for example, the government taking a payment from eBay to allow eBay to continue facilitating transactions involving contraband.

114. We discuss below in the context of child pornography the difficulties of regulating material that appears at a site without a stable domain name and IP address. That possibility raises a technological question of great importance to the regime suggested here. Suppose, for example, that imposition of any of the regimes discussed here would lead sites that sell contraband to shift to a model in which their IP addresses are highly unstable, and also suppose that it is not practical for payment intermediaries to filter their transactions in a way that identifies the sites with unstable IP addresses. If that were so, then it might be impractical for payment intermediaries to respond effectively to claims related to contraband. It is our impression—admittedly a contingent impression subject to change as technology develops—that neither of those assumptions are correct.

115. See Mann, *supra* note 48, at 681.

from making payments to sites that sell contraband or counterfeit goods would make it relatively difficult for those sites to survive.¹¹⁶ The biggest problem is the difficulty that the payment intermediary might face in identifying the targeted transactions.

Collectively, those features tend to suggest that the payment intermediary is a relatively ineffective target for responsibility for the counterfeit goods discussed above, where the auction intermediary might be best placed to identify the illicit transactions. At the same time, in areas where regulators can identify sites dominated by unlawful purchases—the salient examples here are the sites selling untaxed cigarettes and unapproved pharmaceuticals—imposition of a hot-list requirement on a payment intermediary might be most effective. In practice, as we see, regulators are becoming increasingly adept at securing voluntary agreements to such requirements, apparently out of the desire of the payment intermediaries to forestall more intrusive and formal regulation.¹¹⁷

2. *Internet Gambling.*—Internet gambling sites allow gamblers to play games or view lines and place wagers on the outcome of everything from poker games and football to the presidential election.¹¹⁸ Not surprisingly, traditional regulation of the primary malfeasors is difficult: Internet gambling websites can be located anywhere in the world, outside the reach of U.S. laws that attempt to regulate them. As with sites from which contraband and counterfeit products are sold, the business model for gambling websites is central to designing an effective regulatory scheme. Because the sites depend on being readily identifiable—pervasive advertising helps to give them offline brand identity—the domain names and IP addresses that they use are relatively stable and

116. That certainly would be true if the remedy extended as well to PayPal. This assumes, as we believe, that at the present time it would impose a substantial constraint on the revenues of an internet retail site for the site to be barred from accepting payments from Visa, MasterCard, and PayPal, largely because existing payment alternatives remain unavailable to most consumers. For a discussion of some of the problems with competing methods of payment, see MANN & WINN, *supra* note 49, at 576–97.

117. One of the most interesting aspects of the problem is the dynamic through which state regulators secure voluntary agreements, apparently operating in the shadow of potentially more onerous formal regulation. Without great detail, the willingness of PayPal to cooperate with state regulators doubtless is attributable to its desire to avoid initiatives that would bring its entire business under regulation as a money transmitter or the like. The willingness of more traditional credit card providers to cooperate is not as easy to understand, given the strong arguments they could bring to bear that the activities of state regulators cannot extend to the activities of national banks permitted by federal regulators. Our sense is that some likelihood of federal support is likely to be important in most situations of effective state intervention. Notice, for example, the participation of the Bureau of Alcohol, Tobacco, and Firearms in the widely noted settlement regarding online tobacco sales, *see supra* note 17. Similarly, as discussed in the section that follows, it is plain that federal policymakers have provided consistent support to state regulatory initiatives aimed at offshore gambling. Our hypothesis is that here, as in the corporate governance area, the resolution of disputes at the state level is directly influenced by the shadow of a potentially more disruptive federal solution. *Cf. Roe, supra* note 25 (discussing the parallel corporate governance dynamic).

118. One website, Tradesports.com, located in Dublin, Ireland, famously offered lines on almost every political race of 2004 (and correctly predicted the winner of every state in the presidential race). *See* George Passantino, *Putting Their Money Where the Votes Are*, S.F. CHRON., Nov. 14, 2004, at B-3.

unlikely to be shared with other sites.¹¹⁹ It also is important that the business model of a gambling site depends directly on making it easy for money to be transmitted to the site.¹²⁰ Our discussion starts with a summary of the existing regulatory scheme (the point of which is to underscore its ineffectiveness) and follows with an analysis of how liability for intermediaries could enhance the effectiveness of regulation.

Under American law, the states are the primary regulators of gambling.¹²¹ This has allowed each state to take an approach to gambling that is more consistent with the mores of the particular state.¹²² This approach allows states to eliminate a large portion of gambling that actually occurs within the state (e.g., an illegal lottery being run from within the state). But states have difficulty preventing activity that occurs outside of their borders, yet involves citizens acting within the state's borders (e.g., a lottery being legally run in one state that illegally solicits customers in another state). In these types of cases, the federal government has stepped in to assist states in enforcing state gambling regulations.¹²³ But generally, the federal government has refrained from exercising its Commerce Clause power to broadly regulate gambling even though the Constitution plainly would permit such regulation in the context of the internet gambling.¹²⁴

Turning to the specific rules for internet gambling, currently no state permits internet-based gambling.¹²⁵ In furtherance of that policy choice, the federal Wire Act (enacted in 1961) outlaws

119. For more on the frequency of shared IP addresses, see Ben Edelman, *Web Sites Sharing IP Addresses: Prevalence and Significance*, at <http://cyber.law.harvard.edu/people/edelman/ip-sharing/> (last updated Sept 12, 2003).

120. *Internet Gambling Funding Prohibition Act*, Hearing on H.R. 4419 Before House Comm. on Banking and Fin. Serv., 107th Cong. (2000) (statement of Gregory A. Baer, Assistant Secretary for Financial Institutions, Department of the Treasury); GAO REPORT, *supra* note 46 at 53 (finding that over 85% of internet gambling websites accept Visa and MasterCard as forms of payment).

121. *See Thomas v. Bible*, 694 F. Supp. 750, 760 (D. Nev. 1988), *aff'd*, 896 F.2d 555 (9th Cir. 1990); *State v. Rosenthal*, 559 P.2d 830, 836 (Nev. 1977); *Chun v. New York*, 807 F. Supp. 288, 292 (S.D.N.Y. 1992) (all holding that authority over gambling was reserved by the states through the Tenth Amendment).

122. For instance, the neighboring states of Nevada and Utah take opposite approaches to gambling presumably because of the distinct cultural differences between the citizens of those states.

123. *See, e.g.*, Act of July 27, 1868, ch. 246, 15 Stat. 194, 196 and Act of September 19, 1890, ch. 908, § 1, 26 Stat. 465, codified as amended at 18 U.S.C. § 1302 (2003) (making it illegal to send newspapers with lottery advertisements and other lottery-related advertisements through the mail). *See generally* G. Robert Blakey & Harold A. Kurland, *Development of the Federal Law of Gambling*, 63 CORNELL L. REV. 923, 931 (1978).

124. *People v. World Interactive Gaming Corp.*, 185 Misc.2d 852 (N.Y. Sup. 1999) (“[T]he Interstate Commerce Clause gives Congress the plenary power to regulate illegal gambling conducted between a location in the United States and a foreign location.”); *see also* GAO REPORT, *supra* note 46, at 12 (“Although gambling regulation is generally left to the states, the federal government has the authority, under the Commerce Clause of the Constitution, to regulate gambling activity that affects interstate commerce. Internet gambling falls into this category, as bets are generally placed at a personal computer in one state or country and received at a server in another state or country.”). It seems plain to us even after *United States v. Lopez*, 514 U.S. 549 (1995), that gambling transactions on the internet would involve interstate commerce even if the personal computer of the gambler and the server were located in the same state, in part because of the likelihood that internet transmissions between those locations would in some part cross state lines and in part because of the close relation between those transactions and transactions that plainly do cross state lines.

125. *See* H.R. Rep. No. 108-133 (2003), stating:

internet gambling,¹²⁶ and thus has been the statute of choice used in the few federal prosecutions of internet gambling.¹²⁷ But it does so by targeting those directly responsible for the gambling, not the intermediaries that merely facilitate it. Thus, under current law, intermediaries that do not knowingly¹²⁸ participate in the gambling activity have no responsibility for it.¹²⁹

a. Targeting ISPs.—The first possibility is to use ISPs to limit internet gambling.¹³⁰ As discussed above, the internet gambling sites tend to be large, stable, and visible operations. And while the Source ISPs can be located outside the reach of U.S. officials, Destination ISPs¹³¹ must have a presence inside the jurisdiction in which their services are offered. Thus, it might seem, Destination ISPs are particularly well suited to assist in limiting access of U.S. residents to gambling websites located abroad. For example, if a Destination ISP is aware of particular gambling sites, it should be able to prevent traffic from their customers from reaching those sites. Requiring the ISPs to block such traffic would tend to be limited to activity that is illegal in the jurisdiction of the customer's ISP; this distinguishes gambling sites from sites like eBay, for

Virtually all States prohibit the operation of gambling businesses not expressly permitted by their respective constitutions or special legislation. Internet gambling currently constitutes illegal gambling activity in all 50 States. Although in June of 2001 the Nevada legislature authorized the Nevada Gaming Commission to legalize on-line, internet gambling operations if and when such operations can be conducted in compliance with Federal law, the Gaming Commission believes that such compliance cannot be ensured at present.

126. The Wire Act states:

Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined under this title or imprisoned not more than two years, or both.

18 U.S.C. § 1084 (2003); *see also* Gottfried, *supra* note 30, at *74–*81 (discussing the application of the Wire Act to internet gambling).

127. GAO REPORT, *supra* note 46, at 11 (“To date, the Wire Act is the federal statute that has been used to prosecute federal internet gambling cases. . .”).

128. The Wire Act applies only to those that “knowingly” use a wire communication facility to assist gambling. 18 U.S.C. § 1084.

129. For discussion of the similar problems other jurisdictions face, see Colin Scott, *Regulatory Innovation and the Online Consumer*, 26 LAW & POL’Y 477, 481–82, 500 (2004).

130. *See* Jack Goldsmith, *What Internet Gambling Legislation Teaches About Internet Regulation*, 32 INT’L LAWY. 1115 (1998).

131. *See supra* subsection II(B)(2)(a).

which the overwhelming majority of transactions are legal.¹³² Thus, regulations that burden the site would have less collateral damage on innocent users of the site.¹³³

At that point, the question becomes one of selecting an appropriate regulatory scheme. Our intuition is to think that this is a case in which a less onerous hot-list scheme makes the most sense. First, it is plausible to think that law enforcement authorities are better placed than ISPs to identify illicit gambling sites. It is not clear that ISPs easily could identify the sites as illicit based on the nature of the transmissions going to and from the sites, while law enforcement authorities could identify them—at least the successful ones—through research with search engines, observance of advertisements,¹³⁴ and the like. Also, because the crime of gambling is in a sense victimless, the object of law enforcement authorities is likely to be to limit the availability of the sites going forward, rather than to ensure that a payment is extracted for each unlawful transaction that has occurred in the past. Thus, a hot-list scheme is likely to serve the felt needs of law enforcement while minimizing the costs to ISPs and thus the costs to innocent customers of the ISPs.

There are, however, significant difficulties with this approach, starting with the difficulty of coordinating multi-state regulation. Assume, for example, that Nevada wishes to permit certain forms of internet gambling that Utah prohibits.¹³⁵ If Utah required its ISPs to block transmissions to and from the sites in question, it is quite likely that customers in Nevada would be adversely affected. Indeed, this type of problem would be inevitable if the ISP's customer base overlapped the state line, absent some technological ability to differentiate the effectiveness of the filter among its customers based on their physical location. Of course, enactment of a single federal regulation would solve much of the problem, largely because of the greater likelihood that all

132. That analysis is open to the strategy that the interloper might open a wide-ranging “Games Bazaar” that involves both legal and illegal activity, the effect of which would be to increase the collateral harm of regulation. Our strong impression is that costs imposed by this kind of tactical design should not “count” as a reason against regulation. And in fact, if the law establishes that such “Bazaars” will be subject to restrictive regulation, then from an ex ante perspective, it would be quite *bizarre* for a rational businessperson to opt for a “Bazaar” structure. For a thorough discussion of using law to alter the scope of bundled products, see Randal C. Picker, *Unbundling Scope-of-Permission Goods: When Should We Invest in Reducing Entry Barriers?*, 72 U. CHI. L. REV. (forthcoming 2005).

133. Such regulation may nevertheless be costly. On November 24, 2004, the World Trade Organization ruled that U.S. law such as the Wire Act violated U.S. commitments to the WTO. World Trade Organization, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/R (Nov. 10, 2004). This case was brought by the Antigua government in defense of its growing internet gambling industry. If the Wire Act is a violation of U.S. WTO commitments, then laws specifically tailored to prevent internet gambling would certainly be found to violate those commitments as well.

134. Our intuition that law-enforcement authorities easily could identify the sites if they wished to do so is based in part on the frequency of radio advertising for illegal internet gambling sites on the leading sports radio station in the city in which we live.

135. This example is given in Gottfried, *supra* note 30, at *76.

customers of United States ISPs would reside in the United States.¹³⁶ To be sure, there is some reason to be wary of rapid federalization of internet gambling,¹³⁷ as a subset of e-commerce, largely because it denies regulators the opportunity to compare the effectiveness of competing approaches.¹³⁸

Another problem is the possibility that such a regulation would violate the First Amendment. As we discuss in more detail in the section on child pornography below,¹³⁹ one federal district court recently held that blocking technology used to implement the Pennsylvania Internet Child Pornography Act violated the First Amendment because the technology led to overblocking—that is, it blocked sites that were not engaged in illegal conduct.¹⁴⁰ As discussed above, gambling sites are much more readily identifiable than pornography sites, and because of their large traffic, at least the successful ones that are important targets are unlikely to share IP addresses.¹⁴¹ Thus, the problem of overblocking is likely to be less serious in this context.¹⁴² It also is relevant that the targeted activity (gambling rather than pornography) is entirely commercial, and thus not nearly so likely to garner First Amendment protection as the pornographic speech discussed below. For those reasons, there is some basis for thinking that the schemes we propose here would satisfy constitutional scrutiny. Still, to the extent the constitutional question remains unclear—and we do not discuss it definitively here—it should give regulators some hesitation in pursuing this strategy.¹⁴³

A final concern is that gambling websites would react to ISP blocking by designing their user interfaces to utilize other technologies not susceptible of IP blocking. Our view is that any such evolution would not place gambling activities outside the reach of ISPs, who would

136. The problem here is a standard one of regulatory symmetry: in practice ISP markets tend to be bounded by national boundaries, which often makes it easier to impose regulations at the national level. See Mann, *supra* note 48, at 706.

137. The problem is complicated by the arguable hypocrisy of state gambling policy, which to an external observer appears to be designed to provide monopoly power in the gambling market to native Americans and government entities rather than to limit gambling based on the harms it causes consumers. The inconsistencies in American policy are part of the reason efforts to target overseas gambling operators have been challenged as inconsistent with American obligations under the WTO. World Trade Organization, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/R (Nov. 10, 2004). See also *supra* note 131.

138. Larry E. Ribstein & Bruce H. Kobayashi, *State Regulation of Electronic Commerce*, 51 EMORY L.J. 1, 67–70 (2002) (discussing inherent problems with federal regulation of electronic commerce such as public choice concerns, bureaucratic inefficiencies, and the prevention of state regulation which may turn out to be a more effective method for regulating the new industry).

139. See *infra* section IV(A)(3).

140. Center for Democracy & Technology v. Pappert, 337 F. Supp. 2d 606, 620 (E.D. Pa. 2004).

141. *Contra* Gottfried, *supra* note 30, at *75 (refraining from distinguishing internet gambling sites from other kinds of websites, 87% of which share IP addresses).

142. *Contra id.*

143. Because of Congress's consistent support of state regulation in this area, we do not discuss the possibility that state regulatory initiatives in this area would violate the dormant Commerce Clause.

nonetheless be required to carry the communication. Rather, blocking techniques may have to adapt as the technologies adapt. For instance, if gambling websites distribute software that connects gamblers directly to the gambling hall, instead of to a website as most business models currently do, then blocking the TCP port utilized by the program is one potential response.¹⁴⁴ The point here is not to convince the reader that any imaginable technological adaptation by gambling websites has a potential ISP blocking response. Rather, the point is that possible evolution by gambling interests is not a justification for refusing to enlist ISPs in regulating internet gambling, especially when foreseeable responses to gambling evolution exist.

To the skeptic that doubts Congress's willingness to step into an area traditionally left to state regulation, we note that Congress recently has considered such legislation: the proposed Internet Gambling Prohibition Act of 2000 would have required ISPs to terminate accounts for those who run internet gambling sites as well as block access to foreign internet gambling websites identified by law-enforcement authorities.¹⁴⁵ Our analysis suggests that such statutes well may be an appropriate response for policymakers that view gambling as imposing a serious social harm.¹⁴⁶

b. Targeting Payment Intermediaries.—The use of payment intermediaries to curtail internet gambling has obvious advantages. As suggested above, the business model for gambling sites depends on ready and convenient facilities for the transmission of funds to the sites. Given the dependence of those businesses on traditional payment intermediaries, it appears that law enforcement authorities could impose a considerable obstacle to the business of those sites through a curtailment of activity from a small number of intermediaries. Moreover, because this would not involve the potential for overblocking discussed above, it is difficult to see any plausible First Amendment challenge. Finally, because a hot-list scheme barring transmissions to internet gambling sites would resemble so closely existing hot-list schemes with which financial

144. This is a response to P2P problems suggested by Solum & Chung, *supra* note 36, at 929–30.

145. H.R. Rep. 106-655 (2000) (“Finally, the bill would impose new mandates on internet service providers (ISPs). H.R. 3125 would require internet service providers to terminate the accounts of customers who run gambling businesses or promote illegal gambling and to block specific foreign gambling internet sites when given an official notice of noncompliance by state or federal law enforcement agencies.”). For a sympathetic discussion of similar legislation, see Goldsmith, *supra* note 130.

146. The problem is complicated by the arguable hypocrisy of gambling policy, which to an external observer appears to be designed to provide monopoly power in the gambling market to native Americans and government entities rather than to limit gambling based on the harms it causes consumers. The inconsistencies in American policy are part of the reason efforts to target overseas gambling operators have been challenged as inconsistent with American obligations under the WTO. World Trade Organization, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/R (Nov. 10, 2004). *See also supra* note 131.

intermediaries already must comply,¹⁴⁷ it seems unlikely that such a scheme would impose costs on them sufficiently substantial to raise the prospect of worrisome collateral effects on law-abiding customers.

Our sanguine view of the use of payment intermediaries is influenced by the extent to which informal efforts directed at payment intermediaries have been successful even without formal legal support.¹⁴⁸ First, many card issuers voluntarily have limited the use of their credit cards for gambling transactions. In the case of Providian, this seems to have been in response to lawsuits by individuals who refused to pay debts incurred at internet gambling sites based on the (dubious)¹⁴⁹ claim that the activity was illegal and so facilitated by the card issuer as to make the debt unenforceable.¹⁵⁰ Other issuers seem to have acted out of broader concerns, including concerns about the credit risk involved in gambling transactions.¹⁵¹ But whatever the reason, those actions apparently have negatively affected the growth of internet gambling enterprises.¹⁵²

More famously, New York Attorney General Eliot Spitzer has been conspicuously successful in convincing payment intermediaries that it is in their best interests not to facilitate internet gambling.¹⁵³ Spitzer gained enormous leverage after winning a case in New York that held New York law applicable to internet gambling regardless of the location of the servers or the

147. See, e.g., DEPARTMENT OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL, FOREIGN ASSETS CONTROL REGULATIONS FOR THE FINANCIAL COMMUNITY (2004) (describing the regulations in place requiring financial institutions to block transactions to individuals and countries), available at <http://www.ustreas.gov/offices/enforcement/ofac/regulations/t11facbk.pdf>.

148. See Gottfried, *supra* note 30, at *86; Scott, *supra* note 129, at 490.

149. See *infra* note 155.

150. See *Providian National Bank v. Haines*, Case No. V980858 (Superior Court, Marin County, California) (Cross-complaint filed July 23, 1998) (making such a claim); Courtney Macavinta, *Providian May Bar Customers from Net Gambling*, at <http://news.com.com/2100-1040-231845.html?legacy=cnet> (Oct. 22, 1999) (explaining the response by Providian to the *Haines* case). See also Gottfried, *supra* note 30, at *82–*85.

151. GAO REPORT, *supra* note 46, at 4:

Full-service credit card companies that issue their own cards and license merchants to accept cards have implemented policies prohibiting customers from using their cards to pay for internet gambling transactions and will not license internet gambling sites. Credit card associations have instituted a different approach—a transaction coding system that enables association members, at their discretion, to deny authorization of properly coded internet gambling transactions. Many major U.S. issuing banks that are members of these associations have chosen to block such transactions because of concerns over internet gambling’s unclear legal status and the high level of credit risk associated with the industry.

152. Charles Crawford & Melody Wigdahl, *Internet Payment Solutions*, in INTERNET GAMBLING REPORT 88–89 (7th ed. 2002) (estimating that internet gambling sites that relied on U.S. gamblers saw their revenues decrease by 35%–40% in 2000, likely as a result of credit card companies’ efforts to stop use of their cards for internet gambling purposes). See GAO REPORT, *supra* note 46, at 4 (“the credit card industry’s efforts to restrict the use of credit cards for internet gambling could, according to research conducted by gaming analysts, reduce the projected growth of the internet gaming industry in 2003 from 43 to 20 percent, reducing industrywide revenues from a projected \$5.0 billion to approximately \$4.2 billion.”).

153. Less famously, the Florida Attorney General followed a similar strategy that was successful in convincing Western Union to refrain from facilitating transactions with internet gambling operations. Gottfried, *supra* note 30, at *86.

registration of the company.¹⁵⁴ Armed with that decision as well as a federal circuit court decision holding that federal law made internet gambling illegal,¹⁵⁵ Spitzer began negotiating with payment intermediaries to encourage them to limit their involvement with internet gambling. Presumably, Spitzer was able to at least implicitly threaten litigation against these payment intermediaries as accomplices in the commission of the illegal gambling activity.¹⁵⁶ But however the pressure was exerted, it was successful. The largest commitment came when Citibank agreed that it would not approve transactions on its credit cards that involve internet gambling websites.¹⁵⁷ A couple of months later, Spitzer entered into an agreement with PayPal that required the company to deny any transactions that it knew involved an internet gambling website.¹⁵⁸ More recently, Spitzer has extended those agreements with commitments from ten additional banks to similarly end approvals for card transactions that involve internet gambling.¹⁵⁹

Again, as with activity of ISPs, Congress has considered (but not yet enacted) legislation targeting payment intermediaries. Specifically, the Unlawful Internet Gambling Funding Prohibition Act¹⁶⁰ would have forbidden payment systems from honoring payments for gambling related services.¹⁶¹ In our view, the very possibility of such a statute casts a shadow over the negotiations among state regulators and payment intermediaries, making it difficult for the intermediaries to withstand plausible requests for cooperation.¹⁶²

* * *

154. *People v. World Interactive Gaming Corp.*, 185 Misc. 2d 852, 858 (N.Y. Sup. 1999) (finding the corporation's personal contacts with New York sufficient to exert personal jurisdiction and apply New York state law to it).

155. *United States v. Cohen*, 260 F.3d 68 (2d Cir. 2001).

156. *Contra e.g.*, *Cie v. Comdata Network*, 275 Ill. App. 3d 759 (Ill. App. 1995), *appeal den.* 662 N.E.2d 423 (Ill. 1996); *In re MasterCard Int'l Inc.*, 132 F. Supp. 2d 468 (E.D. La. 2001); *Jubelirer v. MasterCard Int'l Inc.*, 68 F.Supp.2d 1049 (W.D.Wis. 1999); *Reuter v. MasterCard Int'l* (4th Cir. Ill. 2001) (all holding that a cardmember's use of credit to fund gambling (in these cases at brick-and-mortar establishments) activities does not mean that the credit card company is involved in gambling or the promotion of gambling). It is important, however, that in the internet context, the activity is both illegal and easily identified as illegal.

157. *In the Matter of Citibank South Dakota, N.A.*, at <http://www.oag.state.ny.us/internet/litigation/citibank.pdf> (June 21, 2002).

158. *In the Matter of PayPal, Inc.*, at <http://www.oag.state.ny.us/internet/litigation/paypal.pdf> (Aug. 16, 2002).

159. *Ten Banks End Online Gambling with Credit Cards*, at http://www.oag.state.ny.us/press/2003/feb/feb11b_03.html (Feb 11, 2003).

160. *See* S. Rep. No. 108-173 (2003); H.R. Rep. No. 108-145 (2003); H.R. Rep. No. 108-133 (2003); H.R. Rep. No. 108-51(I) (2003); H.R. Rep. No. 107-339(I) (2001); H.R. Rep. No. 106-771(I) (2000) (all considering the Unlawful Internet Gambling Funding Prohibition Act, which targeted payment intermediaries).

161. *See* S. Rep. No. 108-173 (2003) ("The bill also would require financial institutions to take steps to identify and block gambling-related transactions that are transmitted through their payment systems."). *See also* Gottfried, *supra* note 30, at *87-*90.

162. Our analysis is limited to the United States. Arthur Cockfield suggests to us that there is at least the possibility that data protection rules like the EU's Data Protection Directive might hinder the lawful cooperation of intermediaries in some countries.

In sum, it is not implausible to target ISPs to limit internet gambling, but regulation of payment intermediaries is likely to be more effective, less likely to involve collateral effects on lawful transactions, and less likely to face complicating legal challenges.

3. *Child Pornography*.—Although the First Amendment has limited the ability of the American legal system to condemn pornography broadly, child pornography has long been condemned and made illegal both in the United States¹⁶³ and around the world.¹⁶⁴ Specifically, the Sexual Exploitation of Children Act of 1978¹⁶⁵ makes it illegal to produce or distribute obscene images of children (originally limited to those under sixteen, but later raised to eighteen¹⁶⁶).

During the 1970s and 1980s, child pornography laws apparently were *relatively* effective, at least in this country, largely because the distribution of pornography required printed material, which was difficult to find and expensive when found.¹⁶⁷ But with the advent of the internet, the distribution of child pornography has become cheaper and less risky.¹⁶⁸ Producers can be anywhere in the world, beyond the reach of law enforcement. The result has been a proliferation of child pornography over the internet.¹⁶⁹

This proliferation began on websites, but more recently has shifted primarily to peer-to-peer (P2P) networks, following the same pattern as music piracy.¹⁷⁰ We emphasize the shift to P2P

163. *New York v. Ferber*, 458 U.S. 747 (1982) (stating that content which depicts children engaged in sexual conduct is “a category of material outside the protection of the First Amendment”).

164. *See* United Nations Convention on the Rights of the Child, preamble, 28 I.L.M. 1448, 4163, U.N. Doc. A/RES/44/25 (Nov. 20, 1989) (“States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent: . . . (c) The exploitative use of children in pornographic performances and materials.”); PHILIP JENKINS, *BEYOND TOLERANCE: CHILD PORNOGRAPHY ON THE INTERNET* 30 (2001) (describing efforts to crack down on the sexual exploitation of children in London in the 1880s and Los Angeles in the 1930s).

165. 18 U.S.C. §2252A (making it illegal to use mail to distribute child pornography or produce child pornography for distribution through the mail).

166. *See* Pub. L. No. 98-292, §§ 5, May 21, 1984, 98 Stat. 205.

167. *See* Katherine S. Williams, *Child Pornography and Regulation on the Internet in the United Kingdom: The Impact on Fundamental Rights and International Relations*, 41 BRANDEIS L.J. 463, 469 (2003) (“Prior to the internet, this backseat for child pornography was possibly justified; in the 1970s and 1980s magazines dealing in the area were difficult to obtain, involving penetrating a complex black-market and were generally expensive. The official clampdown had reduced the trade considerably.”); *File-Sharing Programs: Child Pornography is Readily Accessible over Peer-to-Peer Networks*, Testimony Before the Comm. on Gov. Reform, House of Reps. (Statement of Linda D. Koontz, Mar. 13, 2003) [hereinafter Koontz Testimony], available at <http://www.gao.gov/new.items/d03537t.pdf> (“Historically, pornography, including child pornography, tended to be found mainly in photographs, magazines, and videos. The arrival and the rapid expansion of the internet and its technologies, the increased availability of broadband internet services, advances in digital imaging technologies, and the availability of powerful digital graphic programs have brought about major changes in both the volume and the nature of available child pornography.”).

168. *Id.*

169. In 2002, there were 26,759 reports of child pornography on websites and 757 incidents of child pornography on Peer-to-Peer networks (a fourfold increase from the previous year). Koontz Testimony, *supra* note 167, at 1.

170. *Id.*

networks, because it reveals a division of business models that distinguishes this policy problem from the ones discussed above: activity on peer-to-peer networks is much more difficult to regulate through intermediaries, because it is more difficult for an ISP to identify and because it often will not require the use of any payment intermediary (because there may be no payment required). To the extent that a substantial shift to P2P networks occurs, it undermines the effectiveness of *any* gatekeeper remedy and thus decreases the relative desirability of such a remedy.

a. Targeting ISPs.—Again, we start with the possibility of targeting ISPs. Here, surely because of the perception that any level of child pornography is a sufficiently serious policy problem to justify substantial regulatory regimes, lawmakers have already moved to enlist the aid of intermediaries in limiting the spread of child pornography. The most prominent legislation is Pennsylvania’s Internet Child Pornography Act of 2002. That law adopted a hot-list regime, under which ISPs are liable for allowing child pornography to be accessed through their services after being notified of the availability of the pornography at a particular site:

An internet service provider shall remove or disable access to child pornography items residing on or accessible through its service in a manner accessible to persons located within this Commonwealth within five business days of when the internet service provider is notified by the Attorney General pursuant to section 7628 (relating to notification procedure) that child pornography items reside on or are accessible through its service.¹⁷¹

Penalties for failing to comply with the requirement escalated from a third degree misdemeanor fine of \$5,000 for the first offense to a third degree felony fine of \$30,000 for the third or subsequent occurrence. These penalties could be quite high if ISPs were unable or unwilling to block access to these sites. But the hot-list system, as opposed to a traditional damages regime, ensured that the ISPs would at least have the opportunity to avoid the fine by blocking access to a particular URL.

In practice, however, it was not nearly so easy for providers to block access as the legislature apparently supposed. The Pennsylvania Attorney General enforced the law against what we would call Destination ISPs.¹⁷² When the ISPs received notice that child pornography could be accessed over their networks, the ISPs typically attempted to comply by filtering their traffic

171. 18 Pa. S.C.A. § 7622 (2004).

172. See *Center for Democracy & Tech. v. Pappert*, 337 F. Supp. 2d 606, 620 (E.D. Pa. 2004) (explaining that the AG subscribed to internet service from AOL, Verizon, WorldCom, Microsoft Network, Earthlink, and Comcast and surfed the web through these services, sending notices to the ISPs as Child Pornography was accessed).

either for IP addresses, DNS entries, or URLs.¹⁷³ In theory at least, any of those approaches might be successful in censoring the targeted content, but each network operates slightly differently and could implement some of the technologies more efficiently than others.¹⁷⁴ In practice, most ISPs used IP filtering because it was the simplest for them to implement.¹⁷⁵ The problem with IP filtering, however, is that a website can keep the same URL and change IP addresses. Because the URL is the information customers remember to find the site, monitoring is wholly ineffective if it permits the site to avoid regulation simply by changing the IP address but not the URL.¹⁷⁶ ISPs *could* respond by routinely checking URLs and updating IP addresses.¹⁷⁷ At the time of that litigation, however, it appeared to be the case that the most cost-effective method of monitoring also was easy to evade.

Another problem is that IP blocking often leads to blocking content that was not targeted, largely because of “virtual hosting,” where one IP address hosts several subfolders to which different URLs are directed.¹⁷⁸ Because of the perception that this so-called “overblocking” resulted in the blocking of protected speech, a district court in 2004 held the statute unconstitutionally overbroad.¹⁷⁹ The court acknowledged that the law did not prescribe a particular method of blocking prohibited content, but noted that the methods reasonably available to the ISPs resulted in blocking a substantial amount of constitutionally protected speech.¹⁸⁰ Additionally, it is clear that the court was influenced by its perception that authorities were implementing the statute with little concern for the potential for unjustified blocking, both through incorrect blocking of sites in the first instance and through failure to remove blocks from sites even after prohibited material had been removed.¹⁸¹ Ultimately, the court concluded that these problems left the law beyond the bounds of regulation permitted by the First Amendment.¹⁸² Moreover, the court even went so far as to hold that the statute violated the dormant commerce

173. *Id.* at 628.

174. *Id.* at 629.

175. *Id.*

176. *Id.* at 632.

177. *Id.*

178. *Id.* at 617–18, 633.

179. *Id.* at 658 (“The operation and effect of this Act is that speech will be suppressed when a court order is issued, and the procedural protections provided by the Act before the order can issue are insufficient to avoid constitutional infirmity.”). The decision follows a line of similar cases invalidating statutes that require ISPs not to provide harmful materials to minors over the internet. *E.g.*, PSINet, Inc. v. Chapman, 362 F.3d 227 (4th Cir. 2004); ACLU v. Johnson, 194 F.3d 1149 (10th Cir. 1999); AML v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997).

180. *Pappert*, 337 F. Supp. 2d. at 637–42, 650–51.

181. *Id.* at 642–43. Zittrain, *supra* note 45, provides a thorough discussion of the technological questions, detailing a number of steps that ISPs or regulators could take to limit the costs of such regulation.

182. *Id.* at 658.

clause.¹⁸³ The court generally reasoned that the local benefits of the statute were so trivial (because the statute could be so easily evaded) that the commerce clause would not tolerate the inevitable burden on other jurisdictions when the blocking affected out-of-state actors.¹⁸⁴

Pappert imposes an unfortunate roadblock on the use of intermediary liability in this area. To be sure, the dormant commerce clause problem is probably not a serious one, both because the decision on that ground seems implausible¹⁸⁵ and because congressional legislation explicitly banning child pornography from the internet (or authorizing states to do so) should not be difficult to obtain. The harder problem is how to deal with the First Amendment problem (which is of course not within Congress's control). It well may be that a regulator that diligently tried to prevent the blocking of valid speech would obtain a better result. Still, at least for the time being it might be that a law that was so well targeted as to satisfy the *Pappert* court would force ISPs to invest significant funds in redesigning their networks to use URL blocking rather than IP blocking.¹⁸⁶ The law also apparently would have to provide for notice to blocked URLs and a mechanism for removing a block from URLs when prohibited speech has been removed. All in all, the costs to ISPs of compliance with such a law are likely to be sufficiently substantial to undermine the net benefits of such a regime, even in the minds of policymakers that view child pornography as a highly serious social problem. Again, advances in blocking technology could change that balance in short order. For now, however, the problems with targeting ISPs seem substantial.

b. Targeting Payment Intermediaries.—A second option for curtailing child pornography over the internet is to target the payment intermediaries that make it profitable for child pornography to be sold over the internet. As discussed above, a significant amount of pornography is distributed through noncommercial transactions.¹⁸⁷ But commercial websites are a major source of child pornography on the internet, providing much of the material that is distributed through noncommercial transactions.¹⁸⁸ Thus, although targeting payment intermediaries would not stop noncommercial distribution of child pornography, it could

183. *Id.* at 661–63.

184. *Id.*

185. For a thorough discussion of the relevant Commerce Clause concerns, see Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 YALE L.J. 785 (2001)..

186. *Id.* at 652.

187. Koontz Testimony, *supra* note 167, at 5 (listing Usenet groups and peer-to-peer networks as principal channels of distribution of child pornography).

188. *Id.* We speculate that the noncommercial distribution of material that is introduced to the internet in proprietary transactions is caused at least in part by the difficulty that the operators of commercial child pornography sites would face in enforcing rights they might have under copyright law to prevent copying of the material.

significantly limit the commercial source of much of the pornography and thus have a substantial effect on the level of wrongful conduct.¹⁸⁹ Indeed, the effectiveness of targeting payment intermediaries might be even greater for child pornography sites than it is for gambling sites. This is true because commercial pornography websites generally require credit card information to be on file before any customer can access the service. The point is that the credit card both ensures payment for the service and verifies the customer's age, to prevent problems that the site would face if it too easily permitted minors to access pornographic material.¹⁹⁰ Thus, there is every reason to think that access to credit card processing is essential to the business of commercial pornography websites.¹⁹¹

Following a hot-list strategy similar to the proposed Unlawful Internet Gambling Funding Prohibition Act, states could pass laws that make it illegal to process credit card transactions from websites that offer child pornography. These laws could instruct Attorneys General to monitor websites and update lists of those websites for which credit card transactions should not be processed.

Although such a law almost certainly would be challenged on dormant commerce clause grounds,¹⁹² any successful litigation probably would result in nothing more than a shift of legislative authority to the federal level: child pornography has so little public support that it is easy to predict that federal legislators would be happy to pass and implement (and take credit for) any statute that would provide an effective remedy for child pornography. Thus, it seems to us, state regulators might be able to obtain cooperation from payment intermediaries even without formal federal intervention.

There is some possibility, which is difficult to assess, that commercial websites could avoid regulation by routing their credit card transactions through secondary companies that handle transactions from many sites. The success of any such scheme hinges on the ability of the merchant to outsmart the efforts of intermediaries to suppress such transactions. Our intuition is

189. We recognize the possibility that a strategy targeted at limiting commercial exploitation of child pornography could lead to an increase in noncommercial P2P-based child pornography. It is plausible, however, that regulators would view the eradication (or mitigation) of commercial exploitation as an important policy achievement whatever the effect might be on P2P exploitation.

190. Pornography websites were channeled into the use of credit cards to verify age in part by the affirmative defense offered by § 231 of the Communications Decency Act. 47 U.S.C. §231(c)(1)(A) ("It is an affirmative defense to prosecution under this section that the defendant, in good faith, has restricted access by minors to material that is harmful to minors by requiring use of a credit card, debit account . . .").

191. See Koontz Testimony, *supra* note 166, at 5–6 (mentioning a child pornography ring that included websites based in Russia and Indonesia (content malfeasors located out of US reach) and a Texas-based firm that provided credit card billing and access service for the sites).

192. See *supra* text accompanying notes 183–184 (describing the holding of the *Pappert* court on dormant commerce clause grounds).

that the intermediaries could defeat those efforts with relatively little difficulty. First, it is a direct violation of Visa and MasterCard rules for transactions to be submitted directly as the transactions of another merchant. Second, with respect to secondary processors (which are permitted to submit transactions for other merchants), Visa and MasterCard already engage in close monitoring, which makes it easy to identify transactions from particular illegal sites.¹⁹³ There remains the possibility of more sophisticated efforts at evading scrutiny. For example, sites might try to change their IP addresses and URLs so frequently as to make it difficult for law-enforcement authorities to maintain accurate hot lists.¹⁹⁴ We believe, however, that the existing tools for monitoring the patterns of merchant transactions (including the patterns of chargebacks—likely to be high at sites that provide adult content) would make any sincere¹⁹⁵ effort at implementation reasonably effective.

It also is relevant that the collateral costs of such an approach would be relatively low. As discussed above, banks are already required to monitor lists and ensure that payments are not made to prohibited entities such as terrorists.¹⁹⁶ Similar procedures for these prohibited payment recipients could be easily plugged into existing structures with little additional costs imposed. Nor is there a great likelihood of chilling valuable social conduct that is adjacent to or easily confused with the targeted conduct: it might be that some adult content that is technically not obscene would be chilled, but regulators are likely to regard the social loss from that chilling as a cost that they are willing to bear.

* * *

In the end, targeting payment intermediaries is unlikely to prevent completely the dissemination of child pornography over the internet, but it could strike at the heart of the commercial industry that profits from it. If a hot-list scheme like the one summarized above in fact would impose a substantial financial barrier for those firms, it seems likely that the regulation could be implemented without substantial collateral harms to law-abiding customers of the

193. We know this from the pleadings in the *Perfect 10* litigation.

194. Although we have engaged in no field research to examine the question, our anecdotal impression from news sources is that the pornography industry seems to differ in this respect from the gambling industry, because gambling sites depend largely on advertising to draw customers, which requires stable domain names, while pornography sites depend largely on access from search engines and links from other sites, which seem to be updated and changed frequently to avoid law-enforcement monitoring.

195. As the staunch resistance in the *Perfect 10* litigation suggests, sincerity of implementation cannot be assumed too readily, given the great profits that the payment intermediaries presently derive from sites that provide adult content.

196. See, e.g., DEPARTMENT OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL, FOREIGN ASSETS CONTROL REGULATIONS FOR THE FINANCIAL COMMUNITY (2004) (describing the regulations in place requiring financial institutions to block transactions to individuals and countries), available at <http://www.ustreas.gov/offices/enforcement/ofac/regulations/t11facbk.pdf>.

intermediaries. It is of course a question for responsible policymakers whether the costs of such a regime can be justified by the potential benefits of imposing those imperfect barriers on the commercial sector of the child pornography industry. Perhaps the most that can be said is that the reforms outlined here should be attractive to policymakers that view commercial child pornography as an important and serious problem.

4. *Internet Piracy.*—One of the main driving forces behind this Essay is the generally myopic focus of the existing literature on copyright piracy as the most salient example of wrongful internet conduct. Accordingly, because so much already has been written about regulatory schemes that respond to that problem,¹⁹⁷ we address the subject only briefly here, focusing on the key points of the analytical framework we set out above in Part III.¹⁹⁸

From that perspective, continuing the progression from the sections above, the most salient feature of internet piracy is the extent to which it has come to be dominated by disaggregated P2P filesharing. The technology of copyright infringement on the internet has evolved rapidly in the last decade. The basic point is that it would be easy to prevent the posting of copyright-infringing material on static websites through vicarious copyright infringement, but peer-to-peer networks shielded networks from copyright infringement claims through the potential protection afforded by *Sony*.¹⁹⁹ Despite that potential shield, Napster was found guilty of vicarious copyright infringement based on the Ninth Circuit's conclusion that the network had the right and ability to supervise the infringing activity.²⁰⁰

Responding to that analysis, modern peer-to-peer networks have eliminated even this element of their culpability by separating networks from software and decentralizing the indexing process.²⁰¹ They have thus shielded themselves from the type of vicarious liability found in *Napster*.²⁰² Moreover, following the lead suggested by Kraakman's analysis of asset insufficiency,²⁰³ networks and ISPs involved in the industry have evolved to become judgment

197. Fashioning a regulatory scheme for copyright piracy also must account for the direct effects of the internet on the nature of the conduct. The main effect of the internet on gambling and pornography has been to facilitate dissemination of activity that remains socially unacceptable. With respect to copyrighted materials, however, the rise of the internet has altered considerably the uses to which copyrighted materials are put, in ways that call into question the continuing propriety of the existing framework and thus complicate vigorous enforcement of that framework.

198. For a recent discussion that focuses directly on the propriety of intermediary liability, see Hamdani, *supra* note 29.

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

200. *See A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

201. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 380 F.3d 1154 (9th Cir.) (refusing to find liability for Grokster even though it aided end-users in copyright infringement because the service was fundamentally different than Napster), *cert. granted*, 125 S. Ct. 686 (2004).

202. *Id.*

203. Kraakman, *Corporate Liability Strategies*, *supra* note 78, at 869.

proof, limiting the effectiveness of sanctions even against the intermediaries. It seems natural to expect as the technology develops that it in practice will be so decentralized as to obviate the existence of any intermediary gatekeeper that could be used to shut down the networks.²⁰⁴

Indeed, efforts to use intermediaries to limit P2P filesharing have been so ineffective—*despite* the industry's victory in *Napster*—that the content industry has turned again to what seems an almost desperate attempt to prosecute individual copyright infringers who make copyrighted material available over peer-to-peer networks.²⁰⁵ At least initially, the content industry was able to prosecute such claims because current peer-to-peer networks and software allow them to capture enough information about individuals who connect to the network to find the infringers and identify the extent of their infringement.²⁰⁶ Without this information, the copyright protectors would not have enough information to file a claim. However, new networks and users have taken steps to avoid liability by simply shielding their identities and libraries so that copyright protectors are unable to gather the information necessary to prosecute their claims.²⁰⁷ And as this evolution of copyright infringement continues, it seems most unlikely that prosecuting individual users will result in an end to the harm.²⁰⁸

In the terms of this Essay, the most plausible intermediary strategy²⁰⁹ is regulation of the ISPs that provides service to the individual user. If these ISPs have notice of copyright infringement by subscribers, which copyright protectors are happy to give, they could be required

204. See generally Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679 (2003) (explaining that peer to peer networks have eliminated the intermediary on which copyright enforcement relies). The most interesting part of Wu's work is the general theme that the cultural source of the great resistance to copyright law has been the tactical error to press claims of enforcement too harshly. This resonates with the backlash phenomenon described by Mark Roe in *Backlash*, 98 COLUM. L. REV. 217 (1998) and extended in *POLITICAL DETERMINANTS OF CORPORATE GOVERNANCE* (2003).

205. See Amy Harmon, *Subpoenas Sent to File Sharers Prompt Anger and Remorse*, N.Y. TIMES, July 28, 2003, at C1. The success of these efforts is debatable. See Brian Hindo & Ira Sager, *Music Pirates: Still on Board*, BUS. WK., Jan. 26, 2004, at 13. In part this is because the adverse publicity those efforts have generated have suggested to most observers that Congress would lack the political will to adopt a vigorous enforcement system that would result in strong or sure punishment for individual filesharers. For an interesting Note on the dangerous, and perhaps unconstitutional, effect of aggregating statutory damages in infringement cases such as these, see J. Cam Barker, *Grossly Excessive Penalties in the Battle Against Illegal File-Sharing: The Troubling Effects of Aggregating Minimum Statutory Damages for Copyright Infringement*, 83 TEXAS L. REV. 525 (2004).

206. See Alice Kao, Note, *RIAA v. Verizon: Applying the Subpoena Provision of the DMCA*, 19 BERKELEY TECH. L.J. 405, 408.

207. Scott Banerjee, *P2P Users Get More Elusive*, BILLBOARD, July 31, 2004, at 5.

208. Perversely, what probably has in fact reduced the frequency of copyright infringement is more crime: using P2P systems subjects a computer to the threat of viruses that are spread inside the files obtained. Wendy M. Grossman, *Speed Traps*, INQUIRER (U.K.), Jan. 14, 2005, at ___, available at <http://www.theinquirer.net/?article=20718> (last visited Jan. 15, 2005). Another dissuasion has been the systematic effort by the recording industry to saturate P2P systems with dummy files that make getting the music a user actually wants quite difficult. See Malaika Costello-Dougherty, *Tech Wars: P-to-P Friends, Foes Struggle*, PC WORLD, Mar. 13, 2003, at ___, available at <http://www.pcworld.com/news/article/0,aid,109816,00.asp> (last visited Jan. 15, 2005) (documenting the practice and attributing it to a company called Overpeer, which is apparently an industry anti-piracy company).

209. There are of course other strategies. *E.g.*, *supra* note 54.

to terminate the service of the customer. Because such a scheme does not require monitoring by the ISPs—but relies wholly on monitoring by content providers—it could be implemented with less cost than schemes that would require the ISP to monitor the conduct of its customers to identify unlawful filesharing—which strikes us as quite difficult under existing technology, and perhaps normatively undesirable in any case.

Interestingly enough, the Copyright Act already comes close to including such a regime in Section 512(i)(1)(A), which withholds the DMCA liability shield from any ISP that does not have a policy of terminating access for customers who are “repeat infringers.” It is not clear to us why content providers have not relied more heavily on that regime in their efforts to target frequent P2P filesharers. Our guess is that the provision is rendered ineffective by the ease with which any individual terminated under that section could obtain internet access with a new provider.²¹⁰

B. Breaches of Security

We close with a brief discussion of a set of internet problems that collectively can be characterized as security harms: viruses, spam, phishing, and hacking. Generally, these are harms that are unique to the internet, because they involve conduct that is motivated by the rise of the heavily interconnected networks of which the internet consists. The harm of these actions is measured by the immense amounts of money spent by end-users to purchase software to avoid these problems, by the time spent repairing damaged computers, and by the lost value of computers slowed or rendered inoperable by these incidents.²¹¹ Because of the rapid technological development in this area, the comparatively nascent regimes for defining the responsibility even of primary malfeasors, and in part because of our relative lack of knowledge in the area, we are much less confident in our ability to discern the relevant policy concerns in these areas than for the content harms we discuss above. We discuss the topic generally only to illustrate two obvious points that our framework suggests for these issues.

1. *Lack of Strong Intermediaries.*—In comparison to the conduct disseminating illegal content that was the subject of the preceding sections, this is not an area where there is nearly so

210. We note that the provision is quite vaguely written and thus would be likely to result in substantial litigation if it ever came into frequent use. Among the most obvious problems is the fact that it offers no guidance as to the meaning of the term “repeat” infringer or as to who is to determine if particular customers “are” in fact repeat infringers. For a discussion of that problem, see Lemley & Reese, *supra* note 54, at 1420-21.

211. One estimate put the total cost of viruses at \$55 billion for 2003. *Compressed Data*, *supra* note 14. There is significant evidence to suggest that these problems are increasing. A recent study, for example, put the total number of Phishing scams in December 2004 at 9,019, an 8,000% increase over the 107 such scams in December of 2003. Brian Krebs, *Tech Heavyweights Agree to Share ‘Phishing’ Data*, WASHINGTON POST.COM, Feb. 14, 2005, at <http://www.washingtonpost.com/wp-dyn/articles/A24065-2005Feb14.html>. See also *Internet ‘Phishing’ Scams Soared in April*, WALL ST. J., May 24, 2005, at B5.

obvious a need for legislative intervention to sanction intermediaries. As the examples above illustrate, the paradigmatic case for the deployment of a strategy of intermediary liability is the case in which primary malfeasors cannot be controlled directly and in which readily identifiable intermediaries exist that readily can control the conduct yet choose not to do so.

The context of security harms differs in two obvious respects from that paradigm. First, it is not at all clear that any intermediary readily can control the conduct in question. Perhaps the actors who are best able to increase internet security are the software manufacturers that develop the applications that make the internet useful. Although it is not impossible to view the software designer as yet another intermediary that could solve harms from viruses, spam, and hacking, we think it is less useful to think of that as intermediary liability than as a rapidly developing species of products liability.²¹²

Looking solely at the intermediaries we identify in section II(B)(2) of this Essay, payment and auction intermediaries are entirely irrelevant in the context of internet security, because of the lack of any payment or sale transaction in the typical security breach. And it seems unlikely that ISPs serving those that introduce viruses and spam into the internet community can control the misconduct, if only because of the difficulty of identifying the transmissions that cause the problem and filtering out the malicious code.²¹³ Similarly, it is not at all clear that ISPs serving the customers victimized by security breaches can solve the problem, again because of the difficulty they face in designing reliable systems for identifying the kind of traffic that creates these harms. Finally, while phishing scams require the use of ISPs to host spoofed content, those ISPs are Source ISPs that can be located anywhere in the world. Whether such spoofed websites are in fact hosted on computers located outside U.S. jurisdictions is an empirical question to which we don't know the answer. But even if it turns out that those ISPs are located within the U.S., targeting them will simply force them to move their operations abroad.²¹⁴ That is not to say that it is impossible to devise effective intermediary-based strategies. It is to say, however, that it

212. Doug Barnes has written a fine note outlining the perverse market incentives that have led to a market failure for secure software. Douglas A. Barnes, *Deworming the Internet*, 83 TEXAS L. REV. 279 (2004).

213. This is not to say that ISPs should not be required to assist law enforcement officials to the extent possible to track those who release malicious code onto the internet. See LICHTMAN & POSNER, *supra* note 28 (arguing for liability that forces such cooperation). But our relatively uninformed view is that it is technologically difficult or impossible for ISPs to filter traffic to prevent the code from being released on the internet in the first place. In contrast, the responses we suggest to combat the harms discussed in the previous sections of this Part involve intermediaries that have the ability to prevent harm in the first instance. For a discussion of the rapidly evolving technological possibilities here, see Zittrain, *supra* note 26.

214. Websites that host some content would likely be liable under a theory of vicarious liability for fraud. Thus, state laws, and perhaps the Wire Act, already target the primary malfeasors of the harm. But this obviously has not solved the problem.

is likely to require a remedy that is categorically more disruptive of the physical and social character of the internet than the remedies that we discuss above.²¹⁵

2. *Market Incentives Already Exist.*—At the same time, market incentives appear to be driving intermediaries limit these kinds of harms. This is clearest with respect to spam, where one of the most prominent service features on which ISPs compete is their ability to protect customers from spam.²¹⁶ The basic point is that security harms generally have the effect of directly harming the customers of those ISPs. Thus, customers generally will value features of ISP service that limit spam. To give another example, phishing threatens the legitimacy of internet commerce. If customers lose faith in the security of internet transactions, either because they are not sure about the true identity of the websites they are visiting, or because they are not confident in their own abilities to engage in e-commerce without inadvertently divulging sensitive information, those customers are likely to stop using e-commerce websites. This threat has led to a concerted effort by industry to combat phishing schemes.²¹⁷ Further, phishing scams have provided motivation for new technologies and new firms to spring up to combat the danger.²¹⁸ This of course is quite different from the contexts discussed above: the customer purchasing child pornography or gambling online would not wish to pay a premium for an ISP service that made it practically impossible for the customer to gain access to sites containing that content.

We do not wish to push this point too far. Doug Lichtman and Eric Posner, for example, have argued with some force that the market forces we discuss here are suboptimal, so that the efforts we identify remain insufficiently vigorous.²¹⁹ To the extent those responses are suboptimal, the case for intermediary liability is stronger, as they recognize.²²⁰ Our point here is only that the markets give some positive motivation in this area, which differs from the gambling and pornography areas, where intermediaries often profit from the misconduct. Those efforts to date certainly have not put ISPs in a position to prevent that misconduct entirely, but they do reflect at a minimum an effort to eradicate the conduct that differs substantially from the response

215. Zittrain, *supra* note 26, emphasizes the potential for highly intrusive—yet effective—actions in this area.

216. Compare, for example, Yahoo Mail's touting of its spam filters at <http://mail.yahoo.com/?intl=us> ("Powerful spam protection: Read only the mail you really want") with Earthlink's spamBlocker software, provided free of charge to Earthlink customers at <http://www.earthlink.net/spamblocker/> ("Is your email inbox crammed with spam? We can help. Our spamBlocker tool eliminates virtually 100% of junk email.")

217. *E.g.* Krebs, *supra* note 211 (noting that Microsoft, eBay, and Visa recently signed agreements to work with a firm that gathers information on phishing incidents).

218. *See id.*; Cloudmark Helps PayPal Deliver "No-Phishing" Solution to its Customers, TMCnet.com, Dec. 16, 2004, at <http://www.tmcnet.com/usubmit/2004/Dec/1102325.htm> (describing a plug-in available for Microsoft Outlook that helps customers identify phishing emails).

219. *See* LICHTMAN & POSNER, *supra* note 28.

220. *See id.*

the typical ISP takes to respond to the possibility that its customers might be purchasing child pornography or gambling online. If it is true that market incentives are driving an appropriately vigorous response, then an overlay of regulation would provide little added benefit, and might even be counterproductive, given the complexities of defining effective remedies that are not highly intrusive.

V. Conclusion

The internet is coming of age. Though at the advent of the internet it may have been necessary to develop laws and policies that protected the fertile ground in which the businesses and technologies of the internet have grown, today the internet has taken hold and permeates our daily lives. And non-internet companies have incorporated the internet into their business models to increase efficiency and customer service. At the same time, however, harm perpetrated over the internet continues to grow each year. The pirates have arrived on the high seas of the online world and the lack of regulation makes their predations all too easy. The time has come for lawmakers to implement sensible policies designed to reign in the pirates while minimizing the impact on law-abiding users of the internet.

As the internet enters the final stage in its development—rules—we suggest that lawmakers carefully reconsider the early policy of the Congress that internet intermediaries should not bear any burden in bringing order to the internet. We believe that this policy ignores essential truths of the online world—that anonymity and porous international borders make targeting primary malfeasors difficult if not impossible. Internet intermediaries, on the other hand, are easy to identify and have permanent commercial roots inside the jurisdictions that seek to regulate the internet. Further, these internet intermediaries are essential to most of the transactions on which the internet pirates rely. When intermediaries have the technology capability to prevent harmful transactions and when the costs of doing so are reasonable in relation to the harm prevented, they should be encouraged to do so—with the threat of formal legal sanction if that becomes necessary.

The internet is indeed at a crossroads in its development. Whether pirates will continue to threaten legitimate users of the internet, or whether the internet will fulfill its potential for helping users live more fulfilling lives depends on the direction lawmakers take in facing the challenges that currently befall the internet. Existing businesses that derive large profits from the misconduct—payment intermediaries with respect to child pornography, for example—may resist reforms vigorously. Conversely, it may be that market forces or informal pressure applied from state regulatory officials may solve many problems without the need for specific legislative

intervention. Alternatively, continuing market pressures may force improved standards of operation that will solve many of the problems that we address. We have no firm conviction about the shape of the final outcome. We offer this Essay only in the hope that it can aid the design of sensible internet regulation.