

October 2005

## The Promise of Internet Intermediary Liability

Ronald J. Mann

Seth R. Belzley  
seth@belzley.com

Follow this and additional works at: <https://scholarship.law.wm.edu/wmlr>



Part of the [Torts Commons](#)

---

### Repository Citation

Ronald J. Mann and Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 Wm. & Mary L. Rev. 239 (2005), <https://scholarship.law.wm.edu/wmlr/vol47/iss1/5>

Copyright c 2005 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.  
<https://scholarship.law.wm.edu/wmlr>

# THE PROMISE OF INTERNET INTERMEDIARY LIABILITY

RONALD J. MANN\* & SETH R. BELZLEY\*\*

## ABSTRACT

*The Internet has transformed the economics of communication, creating a spirited debate about the proper role of federal, state, and international governments in regulating conduct related to the Internet. Many argue that Internet communications should be entirely self-regulated because such communications 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 largely on the unexamined view that Internet activity is fundamentally different in a way that justifies broad regulatory exemption. At the same time, some kinds of activity that the Internet facilitates undisputedly violate widely shared norms and legal rules. State legislatures motivated by that concern 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 Article 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, this Article discusses how to regulate Internet-related activity in a way*

---

\* Ben H. and Kitty King Powell Chair in Business and Commercial Law, University of Texas School of Law; Co-Director of the Center for Law, Business and Economics University of Texas. Professor Mann earned his J.D. in 1985 from the University of Texas. For comments on earlier drafts, the authors would like to 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, as well as Cam Barker, Doug Barnes, Oren Bracha, Nick Bunch, Arthur Cockfield, Assaf Hamdani, Doug Lichtman, Allison Mann, Travis Siebeneicher, Doron Teichman, and Jay Westbrook.

\*\* Associate, Hogan & Hartson, L.L.P. Mr. Belzley earned his J.D. in 2005 from the University of Texas where he was a Fellow in the Center for Law, Business and Economics at the University of Texas during the 2004-2005 academic year.

*that is consistent with approaches to analogous offline conduct. The Article also assumes that the Internet's most salient characteristic 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 with 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. Over time, 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 intermediary's level of involvement in the challenged conduct.*

*This Article argues 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 Internet's rise has brought about three changes that make intermediaries more likely to be least cost avoiders in the Internet context than they previously have been in offline contexts: (1) an increase in the likelihood that it will be easy to identify specific intermediaries for large classes of transactions, (2) a reduction in information costs, which makes it easier for the intermediaries to monitor the conduct of end users, and (3) increased anonymity, which makes remedies against end users generally less effective. Accordingly, in cases where intermediaries can feasibly control the conduct, this Article recommends serious attention to the possibility of one of three different schemes of intermediary liability: traditional liability for damages, takedown 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.*

*Part III of this Article uses that framework to analyze the propriety of intermediary liability for several kinds of Internet-related misconduct. This Article is 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, selecting a particular level of regulation should depend on policymakers' view of the net social benefits of eradicating the misconduct, taking into account the intermediaries' and innocent users' compliance costs associated with the regulation. Still, the analysis of this Article 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 regulatory scheme's effectiveness, thereby 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 of the difficulty illicit actors have in relocating to new payment vehicles. Third, with respect to security harms, such as viruses, spam, phishing, and hacking, this Article concludes that the addition of intermediary liability in those cases is less likely to be beneficial because market incentives appear to be causing intermediaries to undertake substantial efforts to solve these problems without the threat of liability.*

## TABLE OF CONTENTS

|  |     |
|--|-----|
| INTRODUCTION .....   | 243 |
| I. THE INTERNET AND MISCONDUCT .....                               | 251 |
| <i>A. The End-to-End Structure of the Internet</i> .....           | 251 |
| <i>B. Internet Actors</i> .....                                    | 253 |
| 1. <i>Primary Malfeasors</i> .....                                 | 253 |
| 2. <i>Internet Intermediaries</i> .....                            | 254 |
| <i>a. ISPs</i> .....   | 255 |
| <i>b. Payment Intermediaries</i> .....                             | 257 |
| <i>c. Auction Intermediaries</i> .....                             | 258 |
| <i>C. Existing (Fault-Based) Liability Schemes</i> .....           | 259 |
| II. LIABILITY WITHOUT FAULT: INTERNET                              |     |
| INTERMEDIARIES AS GATEKEEPERS .....                                | 265 |
| <i>A. The Basic Premise</i> .....                                  | 265 |
| 1. <i>The Nature of Gatekeeper Liability</i> .....                 | 265 |
| 2. <i>Gatekeeper Liability and the Internet</i> .....              | 267 |
| <i>B. Variations on the Theme</i> .....                            | 269 |
| <i>C. A Framework for Analysis</i> .....                           | 272 |
| III. APPLICATIONS TO SPECIFIC TYPES OF CONDUCT .....               | 275 |
| <i>A. Dissemination of Content</i> .....                           | 275 |
| 1. <i>Trafficking in Contraband and Counterfeit Products</i> ..... | 276 |
| <i>a. Targeting Auction Intermediaries</i> .....                   | 277 |
| <i>b. Targeting Payment Intermediaries</i> .....                   | 279 |
| 2. <i>Internet Gambling</i> .....                                  | 281 |
| <i>a. Targeting ISPs</i> .....                                     | 284 |
| <i>b. Targeting Payment Intermediaries</i> .....                   | 288 |
| 3. <i>Child Pornography</i> .....                                  | 291 |
| <i>a. Targeting ISPs</i> .....                                     | 292 |
| <i>b. Targeting Payment Intermediaries</i> .....                   | 295 |
| 4. <i>Internet Piracy</i> .....                                    | 298 |
| <i>B. Breaches of Security</i> .....                               | 302 |
| 1. <i>Lack of Strong Intermediaries</i> .....                      | 302 |
| 2. <i>Market Incentives Already Exist</i> .....                    | 304 |
| CONCLUSION .....   | 306 |

## 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 Internet's commercialization in 1994 and its rapid growth since then 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.<sup>1</sup> Using examples that start with the fifteenth century reign of Prince Henry, "the Navigator of Portugal," and continue through the rise of the Internet in the twentieth century, she discerns four phases through which the society that exploits those discoveries commonly passes: innovation, commercialization, creative anarchy, and rules.<sup>2</sup> The phase of innovation is the flash point of discovery. Morse's invention of the telegraph provides an example.<sup>3</sup> 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. For example, Spar discusses the pirates who exploited the newly discovered Atlantic trade routes in the seventeenth century.<sup>4</sup> 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.<sup>5</sup> Spar's best example of that phase is from the early years of radio broadcasting, when competing and wholly unregulated radio stations broadcasted on overlapping frequencies, thereby making any station difficult for listeners to hear.<sup>6</sup> The final phase, the rules phase, follows ineluctably as the commercial enterprises unable to suppress anarchy on their own call upon government

---

1. DEBORA L. SPAR, *RULING THE WAVES: CYCLES OF DISCOVERY, CHAOS, AND WEALTH FROM THE COMPASS TO THE INTERNET* 10-11 (2001).

2. *Id.* at 11 ("[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 157-59.

intervention as the best vehicle to bring order and profit to the wild frontier.<sup>7</sup>

Using that framework, the Internet is in the midst of the third phase. Numerous examples exist of early actors whose businesses have provided a major impetus for the Internet's growth. A set of legal rules also exists 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 the Communications Decency Act (CDA)<sup>8</sup> and the Digital Millennium Copyright Act (DMCA)<sup>9</sup> granted Internet Service Providers (ISPs), the protection from new taxation the Internet Tax Freedom Act granted,<sup>10</sup> 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 those exemptions disadvantage them, 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 Article considers how to implement regulatory regimes that are better suited for the Internet context.<sup>11</sup> The basic problem is that although the Internet undeniably has brought increased efficiency to American firms, eased communication among distant friends, and changed how we shop, book travel arrange-

---

7. *Id.* at 18-22.

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

9. 17 U.S.C.A. § 512 (2004) (exempting ISPs from liability for monetary relief for the transmission of materials that infringe copyrights).

10. Internet Tax Freedom Act, Pub. L. No. 105-277, tit. 11, 112 Stat. 2681-719 (1998). This moratorium on taxing Internet access has been extended twice since its original enactment, most recently in December 2004 as the Internet Tax Nondiscrimination Act, Pub. L. No. 108-435, 118 Stat. 2615 (2004). State and local taxation of Internet access services will thus be prevented through at least October 2007. See *Bush Signs IDEA, Internet Tax Bills*, CONGRESS DAILY, Dec. 3, 2004, at 8. For general discussion of the Internet Tax Freedom Act, see Arthur J. Cockfield, *Designing Tax Policy for the Digital Biosphere: How the Internet Is Changing Tax Laws*, 34 CONN. L. REV. 333, 363-65 (2002); *U.S. House Clears Tax Ban on Internet Service*, WALL ST. J., Nov. 22, 2004, at A8.

11. Of course, the first question in each instance is why the harmed businesses cannot solve the problems on their own. For example, no matter how annoying it might be, why should the government regulate unsolicited commercial e-mail given the obvious market pressures spurring the major ISPs to disable those who send it? That question motivates the skepticism this Article expresses about such regulation in Part III.B.

ments, and provide and enjoy entertainment, 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, the 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 reporter and law review pages have been devoted to finding ways to prevent Internet piracy. Nevertheless, Internet piracy continues and promises to recover from its recent dip,<sup>12</sup> as software developers and users adapt and evolve to avoid the legal regime's current attempts to control their activities.

Piracy is not this Article's focus, in part because the eradication of piracy would require an exercise more in the vein of social engineering than in legal reform.<sup>13</sup> Rather, this Article's focus is on a number of the Internet's other common uses for unlawful purposes that have attracted much less attention. For example, each day gamblers physically present in jurisdictions that outlaw gambling

---

12. In fact, some industry experts suggest that the efficacy of Recording Industry Association of America (RIAA) lawsuits is 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 evidence also exists that lawsuits are effecting long-term successes in some cases. See *File-Sharing Website Ceases Operations*, L.A. TIMES, Dec. 21, 2004, at C3 (reporting that entire websites that hosted links to a popular file-sharing program called Bit Torrent were completely shutting down after lawsuits were filed against one hundred operators of such sites). It remains to be seen, however, if the Bit Torrent system will recover from this setback. Indeed, less centralized means of locating torrents (the files necessary for downloading content) have already emerged. See SuperNova.org – Universal BitTorrent Source, <http://www.supernova.org> (last visited Sept. 18, 2005) (offering a link to software called eXeem, which allows BitTorrent users to find torrents over an independent network). This evolution is familiar. See *infra* notes 220-24 and accompanying text.

13. Many would argue that this is a case where the underlying business models must shift to meet the regulatory regime's limitations. Indeed, there is reason to believe that there is a substantial upside to the business models that the Internet facilitates. See JOHN ALDERMAN, SONIC BOOM: NAPSTER, MP3, AND THE NEW PIONEERS OF MUSIC 185-87 (2001) (listing some of the new business possibilities that have been sparked by the growth of online music sharing); Chris Anderson, *The Long Tail*, WIRED, Oct. 2004 (describing how the ability to provide broader product offerings gives electronic commerce merchants the ability to extract profits from books, music, and movies that could not profit in an offline retail environment), available at <http://www.wired.com/wired/archive/12.10/tail.html>.



bet millions of dollars on card games and sports matches. Although Internet use arguably does not affect the illegality of that gambling,<sup>14</sup> 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 more difficult, leading to the proliferation of material such as child pornography. Similarly, the anonymity that the Internet fosters has made it easier to buy and sell counterfeit goods, pharmaceuticals that are not lawfully available in the jurisdiction of purchase, and other forms of contraband. Moreover, Americans spend billions of dollars and millions of hours each year combating computer viruses spread over the Internet.<sup>15</sup>

Although the Internet has improved our lives in dozens of ways, it has also given rise to detrimental behavior that has proven hard to constrain. Controlling that conduct without restraining the Internet's potential is surely a worthy goal. This Article suggests that the impulse to respond to those problems inevitably involves ISPs and other Internet intermediaries, chiefly payment intermediaries (PIs), such as PayPal, and auction intermediaries, such as 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 who use its system,<sup>16</sup> 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 Internet's rise presents regulators with new challenges by making it easier for illicit actors to conceal their identities and to locate themselves in jurisdictions beyond the reach or influence of U.S. law enforcement officials.<sup>17</sup>

---

14. See *infra* notes 12-28.

15. One estimate put the total cost of viruses at \$55 billion for 2003. *Compressed Data*, TORONTO STAR, Jan. 17, 2004, at D4 ("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.").

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

17. For an interesting discussion of jurisdictional issues created by the multinational character of the Internet, see Joel Reidenberg, *Technology and Internet Jurisdiction*, 153 U. PA. L. REV. (forthcoming 2005) (discussing the attacks by Internet companies on jurisdiction and arguing that technology will make personal jurisdiction more clear as computers become

Meanwhile, Internet intermediaries often play critical roles in the illicit behavior that frustrates regulators. Indeed, Internet intermediaries often profit directly from transactions that effectively would be banned in an offline environment. Of course, policymakers have not been blind to the possibility of employing Internet intermediaries to control their customers' misconduct. As early as 1995, a task force created by President Clinton suggested imposing strict liability on ISPs as a means for controlling some of the Internet's dangers.<sup>18</sup> More recently, state attorneys general and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) reached an agreement with major credit card companies to prevent the processing of payments for illegal Internet cigarette sales.<sup>19</sup> Similar initiatives have been proposed in Congress to address the problem of online sales of prescription drugs,<sup>20</sup> and Pennsylvania passed a statute that but for being held unconstitutional would have required ISPs to block access to child pornography sites.<sup>21</sup> Private parties have pursued intermediaries under principles of tort law. For example, in recent suits against Grokster<sup>22</sup> and eBay,<sup>23</sup> plaintiffs have

---

more interdependent, and as technology more readily allows Internet companies to purposefully avail themselves of a jurisdiction).

18. See BRUCE A. LEHMAN & RONALD H. BROWN, INFORMATION 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>.

19. See *New York Hits Online Sellers of Cigarettes*, N.Y. TIMES, Feb. 12, 2005, at B1 (describing New York State's efforts to combat online cigarette sales); Press Release, Bureau of Alcohol, Tobacco, Firearms and Explosives, Attorneys General and ATF Announce Joint Initiative with Credit Card Companies to Prevent Illegal Cigarette Sales Over the Internet (Mar. 17, 2005), <http://www.atf.gov/press/fy05press/031705Internetcigsalesinitiative.htm>. These agreements have proved to be extremely effective. Bob Tedeschi, *Now that Credit Card Companies Won't Handle Online Tobacco Sales, Many Merchants Are Calling It Quits*, N.Y. TIMES, Apr. 4, 2005, at C5.

20. See Gilbert M. Gaul & Mary Pat Flaherty, *Google to Limit Some Drug Ads*, WASH. POST, Dec. 1, 2003, at A1.

21. See *infra* notes 181-200 and accompanying text.

22. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd.*, 125 S. Ct. 2764 (2005) (finding third-party liability for copyright infringement against manufacturers who distribute a product with the object of promoting infringing uses of the product).

23. *Hendrickson v. eBay Inc.*, 165 F. Supp. 2d 1082, 1094 (C.D. Cal. 2001) (finding that eBay was protected under section 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).

directed their attention to Internet intermediaries in trying to curtail conduct that has detrimental effects on their businesses.

Thus far, however, the law has failed to respond in a way that effectively regulates the activity of the intermediaries. On the contrary, as discussed above, to the extent that Congress has addressed the question, it has designed laws to insulate the intermediaries from liability.<sup>24</sup> State regulators have been considerably more aggressive, but, as this Article discusses, much of the existing formal legislative activity has either fallen in the face of litigation<sup>25</sup> or has encountered problems with coordinating efforts among multiple jurisdictions.<sup>26</sup> Hopefully, this Article's focus on the costs and benefits of regulation can guide regulators in developing nuanced and context-specific rules that are more likely to withstand judicial attack. Recognizing the differing constituencies and aims of state and federal regulators,<sup>27</sup> this Article's analysis also should 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, this Article will illuminate the just concerns of technologists trying to preserve the Internet's generative potential, with a view to facilitating intervention that is more sensitive and less blunt.<sup>28</sup> Thus, among other

---

24. 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 R. Reidenberg, *States and Internet Enforcement*, 1 U. OTTAWA L. & TECH. J. 213, 223-25 (2003) (noting the early exemptions for Internet intermediaries and the need to look for enforcement mechanisms directed at intermediaries).

25. The most salient example is *Center for Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 663 (E.D. Pa. 2004) (invalidating a Pennsylvania statute that targeted 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.

26. Compare, for example, the relative success states have had in regulating cigarette sales, see *supra* note 19 and accompanying text, with the persistent difficulty that Massachusetts has encountered in enforcing its unusual though plainly legitimate weapons law; see Press Release, Massachusetts Attorney General, AG Reilly Obtains Court Order Prohibiting Online Sales by Weapons Dealers (Sept. 10, 2004) (discussing repeated lawsuits directed at online weapons dealers), <http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1289>.

27. 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. 2491 (2005).

28. For a general discussion of the risks of unduly intrusive intervention, see Jonathan

things, this Article's analysis evinces a general preference for initiatives that grant safe harbors to intermediaries in response to specifically defined conduct rather than generally imposing liability.<sup>29</sup>

Scholars have followed up on those possibilities in a variety of ways. Doug Lichtman, for example, has argued in coauthored 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.<sup>30</sup> Although sympathetic to much of Lichtman's analysis, this Article takes a different tack because it largely jettisons the traditional tort principles on which Lichtman builds. In this Article's 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 this Article proposes. As this Article illustrates, a focus on traditional tort law notions of fault necessarily diverts attention to subjective normative questions of blame and responsibility, and away from the more proper 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

---

Zittrain, *The Future of the Internet—and How to Save It* (2005) (unpublished manuscript, on file with authors). For a few current examples, see Katie Dean, *Techies Blast Induce Act*, WIRED, July 23, 2004 (discussing the proposed Inducing Infringements of Copyright Act, S. 2560, 108th Cong. (2004), that would impose liability on manufacturers of devices that "induce" users to engage in illegal filesharing), available at [http://www.wired.com/news/politics/0,1283,64315,00.html?tw=wn\\_tophead\\_2](http://www.wired.com/news/politics/0,1283,64315,00.html?tw=wn_tophead_2); Michael Geist, *Do We Want FCR-Based, Surveillance-Ready Web? Say No to Big Brother Plan for Internet*, TORONTO STAR, Mar. 7, 2005, at D1 (decrying Canada's proposed "lawful access" initiative, which would require all ISPs to facilitate real-time interception of Internet communications).

29. 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 Press Release, National Association of Attorneys General, Kansas Attorney General Carla Stovall Testifies on Illegal Online Pharmacies, State-Federal Cooperation to Protect Consumer (undated), [http://www.naag.org/legislation/stovall\\_online\\_pharm.php](http://www.naag.org/legislation/stovall_online_pharm.php) (last visited Sept. 21, 2005). More recent efforts against intermediaries presage analogous legislative initiatives against the intermediaries. See Gaul & Flaherty, *supra* note 20, at A1.

30. Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395, 404-05 (2003); Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable* 3 (Univ. Chi. L. Sch., John M. Olin Law & Econ. Working Paper No. 217, 2004), <http://www.ssrn.com/abstract=573502>.

problems with imposing strict liability on ISPs for cyberwrongs.<sup>31</sup> Similarly, Kumar Katyal's work on cybercrimes discusses the possibility of imposing liability on ISPs as a response.<sup>32</sup> Generally, however, that literature has failed to understand how the tailoring of remedies to particular contexts can alter or remove many of the most salient and powerful problems with intermediary liability. 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 no gatekeeper liability should exist in cases in which a damages regime is too costly.<sup>33</sup> As explained in Part II.B, other operationally less intrusive regulatory alternatives exist, such as takedown regimes and "hot list" schemes, which in many contexts might vitiate the costs that justifiably concern Hamdani. Similarly, Katyal's perceptive discussion focuses on the idea that principles of "due care" should guide regulation of intermediaries.<sup>34</sup> He does not recognize that effective regulation of intermediaries must leave concepts of "due care" behind.

In sum, this Article's basic thesis is that the time has come for the Internet to grow up and for Congress and the businesses that rely on the Internet to accept a mature scheme of regulation that limits the social costs of illegal Internet conduct in the most cost-effective manner.<sup>35</sup> Part I of this Article sets the stage by describing the Internet's technological structure, the actors who serve as intermediaries, and the existing liability regimes, which are largely fault-based. Part II describes a new proposal, which rests entirely on the economic principle of identifying the least-cost avoider. In a consciously exceptionalist<sup>36</sup> argument, this Article argues that

---

31. Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901, 916-21 (2002).

32. Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1095-101 (2001). For a similar discussion of Internet gambling, see Jonathan Gottfried, *The Federal Framework for Internet Gambling*, 10 RICH. J.L. & TECH. 26, ¶¶ 74-81 (2004), <http://law.richmond.edu/jolt/v10i3/article26.pdf>.

33. 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 31, at 934-35.

34. Katyal, *supra* note 32, at 1095-101.

35. This is a sentiment that is quickly gaining favor among scholars. *E.g.*, Michael Geist, *Revise Rules to Foster Competition, Protect Privacy*, TORONTO STAR, Mar. 21, 2005, at C3.

36. Although this Article's argument tends to suggest special rules for the Internet, Part

specific characteristics of the Internet make intermediary liability relatively more attractive than it has been in traditional offline contexts because of the ease of identifying intermediaries, the relative ease of intermediary monitoring of end users, and the relative difficulty of directly regulating the conduct of end users. This Article then discusses the circumstances when intermediary liability will be practical, and the characteristics that differentiate the desirability of the 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 facilitating transactions with certain parties. Finally, Part III applies the proposal to four types of content harms—contraband, gambling, child pornography, and piracy—and to the general category of security harms. Although previous writers have discussed extensively the pros and cons of imposing liability on intermediaries related to piracy, relatively little attention has been focused on the role intermediaries can play in other contexts, and almost no attention has been focused on the specific features of intermediaries and their particular businesses, which make regulation in particular contexts more and less effective.

## I. 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. Originally, the United States Government conceived of and designed the Internet for use by the military and university researchers.<sup>37</sup> When use of the Internet was

---

II.A justifies those special rules by grounding them in specific features of the Internet. As the discussion below should make clear, this Article is generally more sympathetic to the view that traditional principles of regulatory analysis are adequate to respond to the Internet's special features. For a forceful argument for applying traditional principles, see Jack Goldsmith in works such as *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1233-37 (1998). Indeed, a principal motivation for this Article is the view that the existing Internet-based exceptions from liability go too far in protecting conduct that would be unlawful in more conventional contexts.

37. See generally JANET ABBATE, *INVENTING THE INTERNET* 36-39 (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

confined exclusively to the military, military contractors, university researchers, or the military itself managed connections between computers. But as the Internet was adapted to public use, private companies emerged to provide the links among private computers connected to the Internet.<sup>38</sup>

Today, the Internet is a web of privately owned networks that communicate using a common computer language called Transfer Control Protocol/Internet Protocol (TCP/IP).<sup>39</sup> When an Internet user requests data over the Internet, the user's request is routed first from the user's computer to the network to which the computer is connected, then across lines to the network that the computer holding the requested content is connected, and finally to the computer that contains the requested content. These separate networks that comprise the Internet could be operated using a number of different transfer languages. The Internet's structure and the common use of TCP/IP for transfer between networks allow these different networks to communicate with each other. Larry Lessig has described this structure as utilizing an end-to-end (E2E) 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.<sup>40</sup> Lessig suggests that this design has strong implications for and even dictates the appropriate types of Internet regulations.<sup>41</sup> This Article agrees with Lessig that regulations which compromise the end-to-end structure of the Internet must be recognized as imposing a cost in the form of restricting future innovations in Internet applications. Rather than viewing the end-to-end principle as inviolate, however, this Article

---

Defense).

38. See *id.* at 195-200.

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

40. LAWRENCE LESSIG, *THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD* 34-35 (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's structure for Internet regulations.

41. See, e.g., Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 942-43 (2001) (arguing that the E2E principle suggests that cable broadband ISPs should not be allowed to force customers to subscribe to particular content in order to receive Internet service).

believes that it is sufficient simply to recognize the costs of intrusive regulations in a larger cost-benefit analysis.<sup>42</sup>

### *B. Internet Actors*

Although previous scholars have built on Lessig's insight by breaking the Internet down into various layers that might be regulated in different ways,<sup>43</sup> this Article takes 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 middle. 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.<sup>44</sup> 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 and are acting to facilitate the actions of end users sending, requesting, and receiving those transmissions. The following Sections provide a crude taxonomy.

#### *1. Primary Malfeasors*

Primary malfeasors offer or receive content or products over the Internet that violate laws relating to copyright, child pornography, gambling, trademarks, and other subjects. A gambling website's proprietor, 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

---

42. For a similar intuition, see Zittrain, *supra* note 28, at 107-08. Canadian regulators have determined that violating the end-to-end principle is justified by the need for regulating Internet conduct. Their "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 by law. See Geist, *supra* note 28. For general information on the Canadian initiative, see SUMMARY OF SUBMISSIONS TO THE LAWFUL ACCESS CONSULTATION (Nevis Consulting Group ed., 2003), [http://canada.justice.gc.ca/en/cons/la\\_al/summary/las\\_report\\_042803\\_e.pdf](http://canada.justice.gc.ca/en/cons/la_al/summary/las_report_042803_e.pdf).

43. See, e.g., Solum & Chung, *supra* note 39; Kevin Werbach, *A Layered Model for Internet Policy*, 1 J. TELECOMM. & HIGH TECH. L. 37, 59 (2002).

44. For example, consider the Canadian "lawful access" initiative. See *supra* note 42.



at the content layer by putting content onto the web that threatens computers with Internet access.

## *2. Internet Intermediaries*

The Internet's early days witnessed many broad claims about how the Internet would lead to widespread disintermediation,<sup>45</sup> 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 Internet's technology 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, with the exception of those relatively few entities sufficiently involved in Internet transmissions to be directly connected to each other. More importantly for this Article's purposes, commercial transactions on the Internet require the use of other intermediaries. In commercial transactions, payment intermediaries must be used, because such transactions cannot use cash as payment. Auction intermediaries are also often employed to bring the parties together. This Article cannot hope to describe *all* the intermediaries that facilitate Internet commerce in the current environment, much less those that will arise in the future. For present purposes, however, a focus on three classes of businesses will be useful. These classes include the most prevalent and interesting types of intermediaries: ISPs, payment intermediaries, and auction intermediaries.

---

45. See, e.g., Andrew L. Shapiro, *Digital Middlemen and the Architecture of Electronic Commerce*, 24 OHIO N.U. L. REV. 795, 795-97 (1998).

*a. ISPs*

ISPs are necessary at every stage of an Internet transaction.<sup>46</sup> 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 provides the physical network that transmits data across the country or the protocols that ensure the data gets routed to the correct place. But recognizing the importance of context sensitivity to appropriate regulatory design, distinguishing different roles that ISPs play in common Internet activities is important.

For this Article's 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, backbone providers, includes those that operate solely at the transmission level, with no direct relationship to any of the actors at the transmission's endpoints. Backbone providers are of relatively little interest to this Article, because of the costs and difficulties involved in configuring their networks to distinguish among the different types of data they carry.<sup>47</sup>

Destination ISPs serve the end user who requests content over the Internet. These ISPs are the entities that bill the end user for Internet service and provide applications such as the ability to

---

46. 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, 63-64 (1998).

47. Earlier writers seem to have taken this view by arguing that the difficulty of understanding the data that travels over ISP networks is an artifact of the Internet's basic transmission protocol, under which such data takes the form of disintegrated packets of any particular file. See LESSIG, *supra* note 40, at 34; Solum & Chung, *supra* note 39, at 829. Commenters on this Article, however, suggest that this perspective is overstated. First, it seems plain that backbone providers can readily discern the IP address to which packets are being routed. More generally, readers of a draft of this Article easily imagined technology that would allow backbone providers to recognize certain types of content passing through its network. As with much of this Article's analysis, technological changes might change the optimal regulatory strategy. Regulation at the backbone level, however, is likely in most cases to involve costs to *all* traffic, which would outweigh the benefits reasonably attributable to the regulation. See Zittrain, *supra* note 28.

connect to the World Wide Web. Thus, they serve as the end users' gateways to everything on the Internet. As the owners of the equipment that operates to link networks to the Internet backbone and that translates 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, such as worms, viruses, or spam.

One premise of this Article is that the current regime's inability to control many of the Internet's harms comes from a myopic focus on the source ISP, the ISP which provides access to the businesses that make unlawful content available.<sup>48</sup> For regulatory purposes, two important distinctions exist 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 multiple ways that are relevant both in assessing the "fairness" of "blaming" the source ISP for the misconduct (the predominant question in existing judicial doctrine) and in assessing how effectively the source ISP can serve as a gatekeeper to stop the misconduct (the predominant question for this Article). For example, a source ISP that provides not only access but also a server on which the unlawful material resides may be better placed to monitor and control the activity than one providing only access.

The second distinction, however, is more important for this Article: a 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, a source ISP willing to facilitate unlawful behavior can remove itself to a jurisdiction that does not prohibit the behavior in question. Thus, for example, a source ISP willing to facilitate Internet casinos can make its services available anywhere local laws allow such activities,<sup>49</sup> putting these entities outside the reach of most law enforce

---

48. Jonathan Zittrain best makes this point. See Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 661-62 (2003).

49. 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 U.S. GEN. ACCOUNTING OFFICE, *INTERNET*

ment agencies.<sup>50</sup> But a destination ISP providing the connection for customers in Ohio to visit an 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 reliably to a seller. For example, when an Internet user incurs a debt, either by shopping on the Internet or visiting sites that charge fees for activities conducted there, 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 he can participate in a game of Internet poker, A must provide the website with some form of security to ensure payment of any gambling debts. 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. In practice, the credit card company or the bank is a necessary actor for A's conduct.

This Article's regulatory analysis depends heavily on particular features of existing Internet payment intermediaries. Most importantly, the market is highly concentrated in the hands of the

---

GAMBLING: AN OVERVIEW OF THE ISSUES 52 (2002) (listing thirty-five of eighty-eight Internet gambling websites as registered in either Antigua or Barbuda, but not reporting the percent of Internet gambling taking place at these sites), *available at* <http://www.gao.gov/new.items/d0389.pdf> [hereinafter GAO REPORT]; Don Yaeger, *Bucking the Odds*, SPORTS ILLUSTRATED, Jan. 8, 2001, at R1 ("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.").

50. Indeed, the United States even brought a suit in the World Trade Organization against the countries of Antigua and Barbuda in an effort to curtail the proliferation of Internet gambling operations on those tiny island nations. The United States lost. *See Herbies Helps Antigua in WTO Outsourcing Victory*, LAWYER, Apr. 5, 2004, at 10. A more recent WTO decision seems to have been broad enough to allow for at least some U.S. regulation of Internet gambling, but that decision certainly stops short of endorsing such regulation. *See Fox Butterfield, U.S. Limits on Internet Gambling Are Backed*, N.Y. TIMES, Apr. 8, 2005, at C14.

dominant credit card networks, and new entrants face high, perhaps insuperable, barriers to entry.<sup>51</sup> At some point, intermediaries that have such a comprehensive command of the market begin to resemble the common carriers on whom lawmakers typically have imposed regulatory obligations in the public interest. To be sure, early predictions were that a new kind of money—generically called electronic money—would be created to facilitate Internet transactions. Still, those technologies have not yet gained any significant base of users, and little reason exists to think they will gain such a user base in the foreseeable future.<sup>52</sup> The most common new payment mechanism for Internet transactions are person-to-person (P2P) systems,<sup>53</sup> such as PayPal, which allow nonmerchant individuals to receive payments, but even that market has rapidly become highly concentrated.<sup>54</sup> For Internet actors with a business model that involves the receipt of money, the concentrated and barrier-protected model provides a highly visible “choke point” for regulatory intervention: an Internet pharmacy in Canada cannot profitably sell pharmaceuticals to U.S. citizens if it does not accept payment devices that U.S. citizens are likely to use.<sup>55</sup>

### *c. Auction Intermediaries*

The last major type of intermediary is the auction intermediary, which matches buyers and sellers through a website that acts as a mediating device to facilitate sales between remote parties. Although other competitors exist, eBay is the dominant and typical player in this multibillion-dollar industry, and thus not surprisingly

---

51. In 2002, more than eighty percent of Internet transactions used credit cards. Ronald J. Mann, *Regulating Internet Payment Intermediaries*, 82 TEX. L. REV. 681, 681 (2004).

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

53. P2P in this context 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.

54. See Mann, *supra* note 51, at 683-84.

55. Recognizing that situation, the Organization for Economic Co-operation and Development (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 J. Cockfield, *Transforming the Internet into a Taxable Forum: A Case Study in E-Commerce Taxation*, 85 MINN. L. REV. 1171, 1257 (2001).

the target of most complaints about failure to act to prevent the auction of illegal goods.<sup>56</sup>

### *C. Existing (Fault-Based) Liability Schemes*

Generally, the primary malfeasor is the actor who can most efficiently prevent 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 who wrote the worm and released it. For Internet gambling to be successful, both a gambler and a gambling website must exist. If either is lacking, the gambling will not occur. 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 the law traditionally has pursued.

But regulation that seeks to prevent misconduct through controlling primary malfeasors is not always effective, particularly when individuals are judgment proof or when 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 who share copyrighted material on the Internet has yet to effectively decrease that type of conduct.<sup>57</sup> The Internet's rise 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 to a jurisdiction outside the influence of concerned policymakers.

When targeting primary malfeasors is ineffective, policymakers must choose between allowing proscribed conduct harms to continue unchecked<sup>58</sup> and identifying alternative regulatory strategies. Generalizing broadly, existing formal policy responses have

---

56. See MANN & WINN, *supra* note 52, at 300, 305-07.

57. 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, 1396-99 (2004).

58. As this Article discusses below, one realistic possibility is that responsible policymakers have settled on a system that declares conduct 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 such an area.

proceeded along two paths, both of which have largely resulted in a relatively broad freedom from liability for intermediaries.<sup>59</sup> First, in a variety of contexts, courts have applied traditional fault-based tort principles to evaluate the conduct of intermediaries. Although instances exist in which relatively egregious conduct has resulted in liability,<sup>60</sup> many if not most of the cases have absolved intermediaries from responsibility.<sup>61</sup> 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 intervened to overrule the cases by granting intermediaries broad exemptions from liability.<sup>62</sup> Because courts have interpreted those statutes broadly, the statutes have the potential to provide considerable protection for intermediaries, even beyond the context that motivated their enactment.<sup>63</sup> Although the parallels are not perfect,

---

59. As this Article emphasizes throughout, regulators in a variety of contexts have reached informal agreements with intermediaries in which intermediaries voluntarily agree to cooperate. Most of those agreements seemingly 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 be one reason why, for example, PayPal—hoping to avoid onerous state licensing requirements—seems to have been more responsive to those efforts than entities like Visa and MasterCard. For a discussion of state regulatory treatment of PayPal, see Mann, *supra* note 51, at 682.

60. See *A & M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896, 911-12 (N.D. Cal. 2000).

61. This Article does not take a view on the correctness of that doctrine but notes it as part of the background that motivates this Article's thesis. For trenchant criticism, see Lichtman & Landes, *supra* note 30 and accompanying text.

62. The most obvious example of this action can be found in the history of the Communications Decency Act (CDA). Congress directly responded to the ISP liability found in *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 23 Media L. Rep. (BNA) 1794 (N.Y. Sup. Ct. May 24, 1995), by including immunity for ISPs in the CDA, 47 U.S.C. § 230(c)(1) (2000) (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. James P. Jenal, *When Is a User Not a "User"? Finding the Proper Role for Republication Liability on the Internet*, 24 LOY. L.A. ENT. L. REV. 453, 459 (2004). Similarly, Title II of the Digital Millennium Copyright Act (DMCA), codified at 17 U.S.C. § 512, settled the tension over ISP liability for copyright infringement committed by subscribers, which the courts created by taking the opposite approach to the issue. 17 U.S.C. § 512 (2000). Compare *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552, 1556-59 (M.D. Fla. 1993) (finding liability), with *Religious Tech. Ctr. v. Netcom On-Line Comm'n Servs., Inc.*, 907 F. Supp. 1361, 1372 (N.D. Cal. 1995) (refusing to find liability).

63. *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); *Gentry v. eBay, Inc.*, 121 Cal. Rptr. 2d 703 (Cal. App. 2002) (holding that the CDA insulates eBay from claims for facilitating the sale of counterfeit goods).

other jurisdictions seem to be taking a similar approach.<sup>64</sup> The paths share not only the reflexive and unreflective fear that recognition of liability for intermediaries might be catastrophic to Internet commerce but also a myopic focus on the idea that the inherent passivity of Internet intermediaries makes it normatively inappropriate to impose responsibility on them for the conduct of primary

---

64. 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.*, 2001 Q.B. 201 (1999), held an Internet service provider liable as the publisher at common law of defamatory remarks posted by a user to a bulletin board. See Mitchell P. Goldstein, *Service Provider Liability for Acts Committed by Users: What You Don't Know Can Hurt You*, 18 J. COMPUTER & INFO. L. 591, 640 (2000) (stating that Parliament was reviewing the decision). In the United States, section 230 of the CDA apparently would prevent such a finding of liability. 47 U.S.C. § 230 (2000). Similarly, courts in France have held ISPs liable for illegal actions of users. In one case, the Tribunal de Grande Instance de Paris held Yahoo! liable for violating a law banning the sale of Nazi objects after users of a Yahoo! auction site posted outlawed materials. See *UEJF & LICRA v. Yahoo! Inc. France*, [T.G.I.] [ordinary court of original jurisdiction] Paris, May 22, 2000, available at <http://www.juriscom.net/txt/jurisfr/cti/yauctions2000522.htm>; see also *UEJF & LICRA v. Yahoo! Inc.*, [T.G.I.] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, available at <http://www.cdt.org/speech/international/00120yahoofrance.pdf> (discussing the order of May 22 and rejecting Yahoo!'s contention that the order could not be carried out because of technological limitations). For a nice summary of the Yahoo! case, see Reidenberg, *supra* note 24, at 215-17.

In 2000, however, the European Parliament passed Council Directive 2000/31/EC, 2000 O.J. (L178) 1, available at [http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l\\_178/l\\_17820000717en00010016.pdf](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.* at art. 12, 13. Further, the Directive forbids member states from imposing general duties to monitor on ISPs. *Id.* at 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*, 23 Media L. Rep. (BNA) 1794, and *Netcom*, 907 F. Supp. 1361. Of course, courts are always free to interpret the Directive or national legislation under the Directive as not applying to the case at hand.

Canada has also passed legislation giving ISPs immunity similar to the DMCA. Canada's Copyright Act states that

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.

R.S.C., ch. C-42, § 2.4(1)(b) (1997) (Can.). The Canadian Supreme Court interpreted this provision 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*, 240 D.L.R. 193, ¶ 92 (Can. 2004). The court in that case also interpreted the statute to require something akin to the DMCA's takedown provision. See *id.* ¶ 110.



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, without regard to their blameworthiness, might be the most effective sources of regulatory enforcement.

The recent litigation involving Perfect 10, Inc. is a salient example of the ineffectiveness of tort principles in imposing liability on Internet intermediaries.<sup>65</sup> Perfect 10 owns copyrights in a large number of arguably pornographic<sup>66</sup> photographs, which it exploits through a printed periodical and a website.<sup>67</sup> Apparently, because of the photographs' significant commercial value, they have appeared regularly on a substantial number of websites without Perfect 10's consent and thus in flagrant violation of Perfect 10's rights under copyright law.<sup>68</sup> The primary defendants' open contempt for intellectual property rights 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, such as Jessica Simpson.<sup>69</sup>

To protect its intellectual property, Perfect 10 instituted several separate causes of action. The most directly responsible defendant was probably Cybernet, a company that operated a system for verifying customers' age by using credit card accounts.<sup>70</sup> Among its various activities, Cybernet operated a consortium of privately run Internet websites that provided pornographic material.<sup>71</sup> To facilitate this network, Cybernet charged customers a monthly fee

---

65. The account of the Perfect 10 litigation in this Article draws not only on the various published opinions in the litigation, but also on pleadings obtained from PACER.

66. The term "pornography" is used loosely in this Article to refer to material marketed with claims of a generally prurient appeal. No effort is made to distinguish 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 III is limited to child pornography so as to avoid the difficult line-drawing questions inherent in the regulation of adult-related businesses more broadly. See *Ashcroft v. ACLU*, 535 U.S. 564 (2002) (consideration of those problems by a divided Court).

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

68. *Perfect 10, Inc. v. Cybernet Ventures, Inc. (Cybernet II)*, 213 F. Supp. 2d 1146, 1163-64 (C.D. Cal. 2002).

69. *Cybernet I*, 167 F. Supp. 2d at 1118, 1125.

70. *Cybernet II*, 213 F. Supp. 2d at 1157-58. The system's utility generally rests on the not entirely accurate assumption that minors are not holders of credit card accounts. See *id.*

71. *Id.* at 1158-59.

and provided those customers with a password that could be used to access more than 300,000 privately run pornographic websites.<sup>72</sup> Perfect 10 claimed that Cybernet was liable for direct, contributory, and vicarious copyright infringement; direct and contributory trademark infringement; and unfair competition.<sup>73</sup> 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 sufficient to justify preliminary injunctive relief on claims for contributory and vicarious copyright infringement, and aiding and abetting unfair competition.<sup>74</sup>

Of more interest to this Article, however, are Perfect 10's actions against Visa, MasterCard, and Google.<sup>75</sup> Perfect 10 claimed, for example, that Visa and other companies that facilitated the credit card transactions were liable for contributory copyright infringement because they enabled Cybernet websites to operate profitably.<sup>76</sup> Among other things, Visa and MasterCard clearly 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.<sup>77</sup> Although unclear from the opinions, the pleadings plainly show that one consequence of placing Cybernet in that category is that Visa and MasterCard charged higher-than-normal fees to Cybernet.<sup>78</sup>

In what seems a perfectly plausible application of existing law, the court had little difficulty in dismissing the action against Visa

---

72. *Id.*

73. *Id.* at 1165-89.

74. *Id.* at 1168-69, 1171, 1174, 1184, 1186-87.

75. 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 turned on details of copyright law that are not interesting for this Article's 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, 1086-103 (C.D. Cal. 2004).

76. *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, No. C04-0371 JW, 2004 WL 1773349, at \*1-2 (N.D. Cal. Aug. 5, 2004).

77. *Id.* at \*2.

78. Complaint at 12-19, *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, 2004 WL 1773349 (N.D. Cal. 2004) (No. C 04-0371 JW).

and MasterCard.<sup>79</sup> The court relied heavily on the content neutrality of Visa and MasterCard services:

Unlike Cybernet, 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 [sic] 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.<sup>80</sup>

These cases should be analyzed quite differently. The approach of the courts exonerates Visa and condemns Cybernet based on the 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, albeit one not readily susceptible to 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 better situated because of the real world likelihood that none of the sites that foster the infringement could survive as a profitable commercial enterprise without accepting Visa payments.<sup>81</sup> This does not mean that Cybernet should be exempt from traditional copyright liability if its participation in the conduct is sufficiently direct, which it seems to be. It does mean, however, that a separate form of liability for Visa and MasterCard should be considered, one that rests not on the degree of passivity but rather

---

79. 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>.

80. *Perfect 10, Inc.*, 2004 WL 1773349 at \*3.

81. This Article assumes that any rule would apply equally to MasterCard, Visa, and the leading payment intermediaries, so that a ruling in favor of Perfect 10 would prevent the sites from accepting payments from any of the dominant providers. To the extent the court erred, it did so in its assumption that a ruling against the payment intermediaries would have no effect on Cybernet's business. *Id.* at \*4. Cybernet would be highly unlikely to survive as a profitmaking entity without access to one of a small number of dominant payment intermediaries.

on the structural relation between the payment providers and the challenged conduct.

## II. LIABILITY WITHOUT FAULT: INTERNET INTERMEDIARIES AS GATEKEEPERS

### A. *The Basic Premise*

This Article's basic premise is that the response described above is a wrong turn. Fundamentally, this Article argues that responding to Internet-related misconduct with rules for intermediaries that turn so pervasively on normative and fault-related notions of responsibility and participation is inadequate. The touchstone this Article suggests—searching for the least-cost avoider—is not novel. Moreover, the idea that in some cases misconduct can be sanctioned most effectively through the indirect imposition of responsibility on intermediaries is also not new. That idea is prominently associated with Reinier Kraakman's two papers written in the 1980s on "gatekeeper" liability.<sup>82</sup> To understand the idea's importance, it is necessary to examine both the gatekeeper regime's distinctive nature and the reasons it is so well suited to the Internet.

#### 1. *The Nature of Gatekeeper Liability*

The first point is the simplest one and the 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 misconduct's social costs and how effectively the intermediary can sanction the misconduct.<sup>83</sup> This does not make imposing liability in cases in which the intermediary is directly involved in the misconduct inappropriate. For example, in *Napster*, one could conclude on a fair assessment of the facts, as the Ninth Circuit did, that Napster

---

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

83. For more on this calculus, see *infra* Part III.

was so involved in unlawful P2P filesharing<sup>84</sup> as to justify imposing liability on Napster for that misconduct.<sup>85</sup> The gatekeeper inquiry, however, would turn on the question of whether Napster could reliably serve to prevent unlawful filesharing. As this Article discusses below, imposing gatekeeper responsibility on Napster would likely have been ineffective because no actions by Napster could possibly have stopped unlawful filesharing.<sup>86</sup>

To put the point affirmatively, the key question for determining the propriety of intermediary liability is the plausibility that the intermediary could detect the misconduct and prevent it.<sup>87</sup> 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 also that they 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 without effecting the underlying misconduct, then the regulation's costs are likely to be a total loss. This suggests that the central factor in assessing the best regulatory strategy must be the market structure of the various intermediaries: intermediaries with sufficient market power to prevent illicit actors from moving to substitutes are better targets than those for whom ready substitutes exist. Thus, continuing with the example above, focusing attention and regulatory resources on entities like Napster, Grokster, and their progeny makes sense only if one could plausibly believe that their eradication would stop piracy. Conversely, attention to the dominant payment intermediaries like Visa and

---

84. This assumes that little personal music trading constitutes fair use under the Copyright Act, 17 U.S.C. § 107 (2000), a conclusion that is not entirely clear.

85. See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1019-23 (9th Cir. 2001).

86. As that discussion emphasizes, this Article does 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. This Article's point is the more systemic one, namely that eliminating Napster and Grokster will do little to slow unlawful filesharing, which in the absence of a significant escalation in the ability of content providers to intervene in the Internet's architecture will continue to proceed on ever more elusive networks. For a cautionary note on the risks of such intervention, see Zittrain, *supra* note 28.

87. Kraakman, *Corporate Liability Strategies*, *supra* note 82, at 889-92; Kraakman, *Gatekeepers*, *supra* note 82, at 53-54.

Mastercard is particularly effective in contexts where the illicit conduct depends directly on access to the facilities of those intermediaries.

The point is not to make a definitive assessment of the potential technological responses, which would be beyond the capabilities of this Article's authors and, in any event, short lived in its accuracy.<sup>88</sup> Rather, the point is simply to emphasize that a strategy utilizing intermediaries makes sense only in contexts where the inevitable costs can be balanced against benefits in real reductions rather than in relocations of misconduct.<sup>89</sup>

## 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.<sup>90</sup> This is true for three reasons. First, as should be clear from the discussion of the Internet's structure in

---

88. For example, one could realistically think that ISPs or even a consumer's own computer soon could be put in a position to monitor the particular applications the ISPs' customers use. See Zittrain, *supra* note 28, at 70-71. If this sounds implausible, consider the conventional wisdom that manufacturers of photocopiers cannot build their machines to prevent private copyright infringement. See, e.g., Lichtman & Landes, *supra* note 30, 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. Obviously it is much easier to build a scanner that recognizes one particular image that it should not copy than it is to produce a copier that can detect any one of millions of copyrighted works. The point is, however, that technological advances should never be underestimated.

89. See Doron Teichman, *The Market for Criminal Justice: Federalism, Crime Control and Jurisdictional Competition*, 103 MICH. L. REV. 1831 (2005) (arguing for a comprehensive structure to the United States criminal justice system to remove competition between local jurisdictions that attempt to relocate crime to neighboring jurisdictions).

90. Joel Reidenberg notes the possibility that intermediary enforcement might be "more efficient" if illegal activities are "channeled through gateway points." Reidenberg, *supra* note 24, at 224. He does not, however, focus as this Article does on the systematic reasons why that might be so.

Part I, a particular type of misconduct on the Internet will often proceed through a readily identifiable intermediary or class of intermediaries, and 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 will interact with a site that describes or provides the contraband and will likely 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 the standard.

Second, advances in information technology make it increasingly cost effective for intermediaries to monitor more closely the activities of those who use their networks. As monitoring activity becomes cheaper, it ineluctably becomes *relatively*<sup>91</sup> more desirable to rely on such monitoring as the least expensive way to eradicate undesirable activity.<sup>92</sup>

Third, the relative anonymity the Internet fosters makes remedies against primary malfeasors less effective than in the brick-and-mortar context. For example, obtaining a relatively anonymous e-mail account from a provider such as Google for use in illicit conduct is easier than obtaining a post office box in the offline world. This is not to say that anonymity is impossible in the offline world or perfect in the online world; engaging in relatively anonymous conduct online is simply easier than it ever has been offline. But, with the introduction of intermediaries in targeting certain activities, this anonymity decreases significantly. The networks intermediaries provide, 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 those networks' users to be identifiable to varying extents. ISPs

---

91. This Article suggests only that it becomes *relatively* more desirable. As emphasized throughout, the costs of monitoring in many cases might make large scale monitoring unjustified except in cases of serious misconduct.

92. This point can be overstated. Just as technology in the last few years seems to have made monitoring easier, technology in the near future will possibly make it easier for wrongdoers to avoid monitoring. As discussed below, this likely 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. However, whether this always will be so is unclear. See Zittrain, *supra* note 28, at 72-73.

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

### *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 intermediary's control. Thus, one of the principal topics in the literature has been the question of whether the liability of the gatekeeper should be strict or based on negligence or fault.<sup>93</sup> A more contextual assessment of the multifarious types of Internet intermediaries, however, suggests that a wider array of policy options should be considered. For present purposes, a description of three types of remedies will suffice: a traditional tort remedy for damages; a takedown regime, such as the DMCA; and a "hot-list" regime, which is 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.<sup>94</sup> If the risk of liability is not readily predictable or cabined, that remedy is likely to have adverse collateral effects, such as overdeterrence.<sup>95</sup> That problem is particularly serious when the remedy applies to misconduct that the intermediary cannot entirely avoid. Consider, for

---

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

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

95. For example, cyberlaw scholars commonly worry that imposing any liability on intermediaries for their customers' actions will lead to the prohibition of anonymous postings, which will have adverse effects on the Internet polity. See, e.g., Henry H. Perritt, Jr., *Property and Innovation in the Global Information Infrastructure*, 1996 U. CHI. LEGAL F. 261, 325.



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 detecting some but not all of the conduct in question feasible for the ISP, then a remedy holding the ISP strictly liable for the misconduct will likely have a considerable adverse effect on *all* users, either through restrictions on service or an increase in price. Conversely, because a damages remedy applies only *ex post*, it would have the undetering aspect of having no effect on the conduct of financially irresponsible intermediaries. The schemes with more objective *ex ante* requirements discussed below 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 DMCA provisions codified in section 512 of the Copyright Act,<sup>96</sup> generally obligate covered intermediaries to remove allegedly illicit conduct promptly upon receipt of an adequate notice of the misconduct.<sup>97</sup> Although this scheme does impose obligations on the intermediaries, it imposes a relatively small risk of liability because it generally carries an implicit exemption from monetary relief if the intermediary complies with appropriate takedown notices.<sup>98</sup> 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 intermediary's aid in identifying and removing illicit material. The dispute between Tiffany & Co. and eBay illustrates the problem.<sup>99</sup> Suppose, as seems likely to be the case, that eBay is

---

96. 17 U.S.C. § 512(c) (2000).

97. *Id.* Such a system of course could be designed more or less effectively. For example, the DMCA may impose 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.

98. *Id.* A possibility, not yet settled in the courts, remains 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, 556 (4th Cir. 2004).

99. 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).

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 rapidly enough to forestall a successful auction. Tiffany might plausibly 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, which 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. In its most common application, banks have for years been prevented from wiring money to any entity on the federal government's list of entities that support terrorist activity.<sup>100</sup> This scheme is likely to provide the most predictable liability 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,<sup>101</sup> violations by the intermediaries might be rare. Of course, this scheme goes 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 criminal transactions begin.<sup>102</sup> Thus, this response will be useful only in

---

100. In response to the terrorist attacks on September 11, 2001, President Bush by executive order made it illegal to transfer property to certain persons listed initially by the Executive Order and subsequently by the Secretary of State. Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001). Today, the Office of Foreign Assets Control, part of the Department of the Treasury, maintains a list of designated foreign nationals for whom banks are forbidden to facilitate transactions. For more on these regulations, see OFFICE OF FOREIGN ASSET CONTROL, FOREIGN ASSETS CONTROL REGULATIONS FOR THE FINANCIAL COMMUNITY 5-43 (2005) [hereinafter OFAC REPORT], available at <http://www.treas.gov/offices/enforcement/ofac/regulations/t11facbk.pdf>.

101. 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 Assets Control, SDN and Blocked Persons, <http://www.treas.gov/offices/enforcement/ofac/sdn/> (last visited Sept. 21, 2005).

102. The text assumes that regulators will not delegate to private entities the ability to designate those 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 would be more costly and thus less justifiable.

situations where the illicit transactions are likely to have a readily identifiable and relatively stable location.

Of course, this Article provides only a simple list of options. One can easily imagine responses that combine features from the various options. Most obviously, the framework above does not specify what the remedy would be for failing to comply with a take down or "hot-list" requirement. The remedy for such a failure could be calibrated to extend only to a loss of immunity, which is 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 that which would be imposed for the illicit activity.

### *C. A Framework for Analysis*

Undoubtedly, the foregoing subparts 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 those who depend on their services. That is not, however, because this Article is unaware of or unconcerned about those costs, but rather because describing the structure and premises of the proposed liability is necessary before this Article 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. The liability schemes that this Article envisions are plainly not the type of thing readily adopted through the development of the common law. This Article's framework is intended to provide fodder for legislators and regulators, not for judges.<sup>103</sup> Hopefully, this Article's 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 possible. As Judge Posner recently explained, such an unbounded principle would be unduly disruptive.<sup>104</sup> In contrast, this Article hopes that

---

103. For analysis criticizing the doctrine judges have developed under the existing statutory scheme for piracy, see Lichtman & Landes, *supra* note 30, at 404-10 (arguing that broad ISP exemptions are inconsistent with traditional rules of tort liability).

104. *Cuyler v. United States*, 362 F.3d 949, 955-56 (7th Cir. 2004).

the state regulators who currently are searching for tools to respond to offensive Internet-related conduct will consult the framework that this Article articulates so that the informal responses that they seek and increasingly obtain will reflect an appropriate sensitivity to the costs their remedies impose.

Furthermore, this Article expresses no views on the social benefits to be gained from eradicating *any* of the various forms of misconduct discussed in Part III. The relevant policymaker should make that judgment call: this Article, for example, expresses no opinion on the relative social benefits to be obtained from limiting the sale of counterfeit goods, the sharing of copyrighted music, and 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.<sup>105</sup> The existing literature focuses on two general categories of costs, which seem illustrative. It is well recognized that imposing liability on intermediaries will affect the services and prices they present to their customers.<sup>106</sup> If regulation increases costs substantially, some customers, such as those who derive net benefits from the service that are less than the newly imposed costs, will stop using the gatekeeper's service. In some cases, and especially as the cost of liability to the gatekeepers increases significantly, the problem may spiral out of control, such that the only remaining customers will be those who use the gatekeeper's services in highly rewarding ways.<sup>107</sup> In situations where the remaining users are predominantly those committing the targeted acts, the regulation's ultimate effects are likely to be counterproductive.<sup>108</sup>

Another problem is that gatekeeper liability might upset the market balance for the services provided by gatekeepers. Specifi-

---

105. For a thorough discussion, see Hamdani, *supra* note 93, at 63-82.

106. See Kraakman, *Corporate Liability Strategies*, *supra* note 82, at 891-92 ("[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."); Kraakman, *Gatekeepers*, *supra* note 82, at 77, 93-94.

107. This is the problem of "unraveling" markets, discussed in detail by Hamdani. See Hamdani, *supra* note 93, at 74-76.

108. *Id.* at 76-80.

cally, a risk always exists that imposing additional burdens on intermediaries will chill the provision of valuable goods and services.<sup>109</sup> That will be especially problematic in cases where considerable risk of chilling legal conduct that is adjacent to the targeted conduct exists. As discussed below, that might tend to make the use of intermediaries less plausible in file-sharing contexts where determining whether any particular act of file sharing is illegal is difficult, and more plausible in the gambling context where in many cases substantially all traffic to a particular site likely involves illegal conduct. Requiring intermediaries to make those kind 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 with positive social value,<sup>110</sup> as is likely in at least some of the contexts this Article discusses, the direct and indirect effects on that conduct must be counted as costs of any regulatory initiative.<sup>111</sup> Thus, this Article emphasizes that in any particular case, the costs of any particular regime described in this Article might exceed the benefits that could accrue from implementing the regime, and in such a case a new regime should not be supported.

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. This is evident 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 of taxable goods and services by business and also through the government's use of the tax revenues.

---

109. *Id.* at 76-77.

110. 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. *Id.* at 73.

111. Sonia Katyal has written extensively on the social costs imposed by section 512 of the DMCA, which she argues copyright holders, frustrated by the difficulty of protecting their property in the digital environment, have used to harass individuals, thus oftentimes curtailing legitimate activity. Sonia K. Katyal, *Privacy vs. Piracy*, 7 YALE J.L. & TECH. 222, 281-90 (2004). These represent one subset of the costs that should be considered when evaluating the costs and benefits of proposed legislation.

In sum, this Article poses 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.

### III. 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 purposes of this Article, two 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 this Article focuses are trafficking in contraband or counterfeit goods, Internet gambling, child pornography, and sharing copyrighted files. The second category includes breaches of security, such as viruses, hacking, and spam, 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 a 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. The analysis in this subpart does not advocate any of these options for the particular types of misconduct that this Article addresses. Rather, this Article's aim is a 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,<sup>112</sup> Tiffany & Co. has been engaged in a long-running dispute with eBay about the sale of counterfeit Tiffany & Co. merchandise on eBay. Other obvious problems, however, have drawn attention from regulators: the sale to U.S. residents of pharmaceuticals that are principally from Canadian retailers<sup>113</sup> and that have not been approved for use by the Food and Drug Administration (FDA), and the sale of cigarettes in violation of local and federal tax laws<sup>114</sup> are notable.

In some ways, these situations are 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 where the sale of the product is plainly illegal.<sup>115</sup> Thus, for example, one could easily see that Massachusetts should be able to proscribe the shipment of firearms to an address physically located in Massachusetts.<sup>116</sup> A rule limited to such shipments would be underinclusive, as it would not bar shipments to addresses outside Massachusetts even if the products ultimately would be distributed in Massachusetts. Additionally, the rule would perhaps be overinclusive, as some shipments to Massachusetts addresses might be intended for use outside the Commonwealth. Yet, a practical scheme for prohibiting such shipments would go a long way, particularly in states larger than Massachusetts, in prohibiting the targeted conduct and would impose relatively little cost on innocent third parties: it is not too much to ask of persons

---

112. See *supra* text accompanying note 99.

113. See Gaul & Flaherty, *supra* note 20.

114. See *supra* note 19.

115. Conduct that does not involve physical shipments is harder to deal with both because of the threshold question of whether the illegal conduct in fact occurs in the targeted jurisdiction (for example, 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.

116. See Press Release, Massachusetts Attorney General, *supra* note 26.

who want to buy guns that are illegal in Massachusetts that they provide a mailing address outside the Commonwealth. Even in cases of nonuniform regulation, such as firearms or wine, the analogy of the Streamlined Sales Tax Project<sup>117</sup> suggests that under current technology, responsible retailers should be able to refrain from shipping contraband into prohibited jurisdictions.

In some cases, however, direct enforcement against a retailer will be ineffective. For example, a jurisdiction might face a large number of small, relatively irresponsible retailers, so that direct enforcement would be prohibitively expensive in practice. Additional examples include cases in which the retailer takes advantage of the relative anonymity an auction site like eBay affords or cases in which the retailer is located in a jurisdiction outside the United States that will not cooperate with the relevant state regulators. Importantly, even in those cases, the business model for the primary malfeasors generally involves a product's retail sale in return for monetary compensation. Among other things, this generally involves the existence of a website where 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. This Article discusses in the next two sections auction intermediaries and payment intermediaries, which seem to be the simplest and most common possibilities.

### *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. In contrast, eBay is an entity with a major domestic presence that owns facilities through which a substantial amount of counterfeit goods are sold. In that context, eBay could clearly detect and prohibit many of the sales of counterfeit Tiffany & Co. products at its site.<sup>118</sup> The real question then is

---

117. See Streamlined Sales Tax Project (Jan. 2005), <http://www.streamlinedsalestax.org/execsum0105.pdf>. For discussion, see Cockfield, *supra* note 10, at 386-88, 397-98.

118. Tiffany & Co. complains of sales of products that are falsely advertised as Tiffany &



whether the burden should be on Tiffany & Co. to locate counterfeit products and bring them to eBay's attention, as under a DMCA take-down regime, or whether the burden should be 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, one could plausibly 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., while eBay probably is not as effective as Tiffany & Co. in distinguishing bona fide Tiffany products from counterfeits.<sup>119</sup> The net benefit of shifting that task to eBay from Tiffany & Co., namely 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 of shifting that task to eBay, on the other hand, are the burdens eBay would impose on all users. Among other things, those burdens are likely to diminish the functionality of eBay's site by setting up additional steps that will slow the availability of innocent users' postings.

If the social benefits of removing the contraband or counterfeit products are high enough, imposing a damages regime might be plausible, 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, however, adopting a takedown regime of some kind might be more plausible, such as a regime under which eBay would be obligated to

---

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 99, at 13. 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 visually search for a particular mark. The development of such a search engine—certainly plausible under existing technology—well might shift the appropriate locus of responsibility.

119. Indeed, assuming that monitoring is the lowest-cost method of eradicating contraband from eBay may be a mistake. For example, circumstances can be imagined in which a lower net burden might be imposed on eBay's business if eBay required bonds from its customers to ensure their compliance with applicable restrictions on contraband. Given the small size and presumptive illiquidity of many eBay merchants, this does not seem to be the optimal response. The main point, however, is that eBay plainly is better situated than Tiffany & Co. in assessing the relative costs of different remedies.

remove all counterfeit products for the owners of famous marks<sup>120</sup> who made a suitable request.<sup>121</sup> Similarly, permitting eBay to impose those costs on the content owner might make sense, particularly if compliance costs would be sufficiently great that they might alter the pricing of eBay's services to all customers. For example, eBay could be permitted to charge content owners, such as Tiffany & Co., a "reasonable fee" for complying with a statutory mandate to remove counterfeit products.<sup>122</sup>

### *b. Targeting Payment Intermediaries*

To the extent that contraband and counterfeit products tend to be sold from a stable site,<sup>123</sup> the payment intermediary also can serve

---

120. This is not as vague as it sounds because "famous marks" is a term of art defined in section 43 of the Lanham Act, 15 U.S.C. § 1125(c) (2000).

121. This would differ from the existing DMCA take-down regime because the notice from the content owner would not identify specific products to be removed, but rather specific marks to be examined.

122. This would more directly link the cost of eliminating the harms to the entity that benefits from their 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 one view the risk to Tiffany & Co. as an externality created by eBay's new business, which eBay should be forced to internalize to ensure that its business increases net social value? From that perspective, one likely view is that it is appropriate to require the trademark owner to pay the reasonable compliance costs to ensure that the private value of the mark exceeds the transaction costs of the takedown. In a perfect world, the baseline would be irrelevant because the trademark owner would negotiate to purchase a takedown from eBay if that were an efficient outcome. Some reason exists to think that might happen where, as in this case, 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 to have significant long-run effects in many contexts on the allocation of investments related to the activity in question. See Lucian Arye Bebchuk, *Property Rights and Liability Rules: The Ex Ante View of the Cathedral*, 100 MICH. L. REV. 601, 605-06 (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. See Ronald J. Mann, *Contracts—Only with Consent*, 152 U. PA. L. REV. 1873, 1896-901 (2004). This problem is much less relevant to the sections of this Article's analysis, such as child pornography and gambling, where the dispute over liability involves 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.

123. This Article discusses 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

a useful role and 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 eighty percent of modern Internet retail transactions use a credit or debit card as a payment vehicle.<sup>124</sup> Furthermore, although precise data is difficult to locate, all of those transactions pass through a small handful of networks, and the lion's share of those transactions taking place in the United States make payment either through the Visa or MasterCard networks. This means that a remedy preventing one of those small number of networks from making payments to sites that sell contraband or counterfeit goods would make it relatively difficult for such sites to survive.<sup>125</sup> The biggest problem is the difficulty a payment intermediary might face in identifying the targeted transactions.

Collectively, those features suggest that the payment intermediary is a relatively ineffective target for responsibility for the counterfeit goods discussed above, especially where the auction intermediary might be better placed to identify the illicit transactions. At the same time, in areas where regulators can identify sites dominated by unlawful purchases, such as sites selling untaxed cigarettes or unapproved pharmaceuticals, imposing a "hot-list" requirement on a payment intermediary might be most effective. In practice, regulators are becoming increasingly adept at securing voluntary agreements to such requirements, apparently out of the payment intermediaries' desire to forestall more intrusive and formal regulation.<sup>126</sup>

---

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 this Article's impression—admittedly a contingent impression subject to change as technology develops—that neither of those assumptions is correct.

124. See Mann, *supra* note 51, at 681.

125. That certainly would be true if the remedy extended to PayPal as well. This assumes that barring an Internet retail site from accepting payments from Visa, MasterCard, and PayPal would impose a substantial constraint on the site's revenues, largely because existing payment alternatives remain unavailable to most consumers. For a discussion of some of the problems with competing payment methods, see MANN & WINN, *supra* note 52, at 576-94.

126. One of the problem's most interesting aspects is the dynamic through which state regulators secure voluntary agreements. They apparently operate in the shadow of potentially

## 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.<sup>127</sup> 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.<sup>128</sup> As with sites selling contraband and counterfeit products, 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 they use are relatively stable

---

more onerous formal regulation. Without going into great detail, the willingness of PayPal to cooperate with state regulators is undoubtedly 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 easily understood, given that they could bring strong arguments that the activities of state regulators cannot extend to the activities of national banks that are permitted by federal regulators. Seemingly, some likelihood of federal support is important in most situations of effective state intervention. Notice, for example, the participation of the Bureau of Alcohol, Tobacco, Firearms and Explosives in the widely noted settlement regarding online tobacco sales. See *supra* note 19. Similarly, as discussed in Part III.A.2, federal policymakers plainly have provided consistent support to state regulatory initiatives aimed at offshore gambling. The hypothesis is that here, as in the corporate governance area, the shadow of a potentially more disruptive federal solution directly influences the resolution of disputes at the state level. Cf. Roe, *supra* note 27 (discussing the parallel corporate governance dynamic).

127. One website, Tradesports.com, located in Dublin, Ireland, famously offered lines on almost every political race of 2004, and incidentally, 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 B3.

128. And this is apparently exactly what Internet gambling companies are doing to ensure financial success. PartyGaming, an Internet gambling website that recently went public in Great Britain, acknowledged in securities documents that the company could be engaging in illegal conduct in some of the countries from which it draws customers. But the company shrugged off the concern, stating, "PartyGaming and its directors rely on the apparent unwillingness or inability of regulators generally to bring actions against businesses with no physical presence in the country concerned." Kurt Eichenwald, *At PartyGaming, Everything's Wild*, N.Y. TIMES, June 26, 2005, at B1. Apparently unconcerned with this spectre of illegality, the market embraced PartyGaming stock, making it one of the largest IPOs in London in recent history. *Id.* Interestingly, the size of the IPO and the subsequent success of the shares indicates that American fund managers are among PartyGaming's investors. Heather Timmons & Eric Pfanner, *Online Gambling Shares Climb 11% in Debut Day*, N.Y. TIMES, June 28, 2005, at C6. This fact may make it very difficult for prospective action against such online gambling companies to gain any traction in the face of what would certainly be sizeable opposition from U.S. interests.

and unlikely to be shared with other sites.<sup>129</sup> Importantly, a gambling site's business model depends directly on making it easy to transmit money to the site.<sup>130</sup> This Article's discussion starts with a summary of the existing regulatory scheme for the purpose of underscoring its ineffectiveness, and follows with an analysis of how liability for intermediaries could enhance the effectiveness of regulation.

Under U.S. law, the states are the primary regulators of gambling.<sup>131</sup> This has allowed each state to take an approach to gambling that is consistent with the particular state's mores.<sup>132</sup> This approach allows states to eliminate a large portion of gambling that actually occurs within the state, such as an illegal lottery being run from within the state. States, however, have difficulty preventing activity that occurs outside their borders but that involves citizens acting within their borders, such as the illegal solicitation of customers in one state by a lottery being legally run in another state. In these types of cases, the federal government has stepped in to assist states in enforcing state gambling regulations.<sup>133</sup> 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 Internet gambling.<sup>134</sup>

---

129. For more on the frequency of shared IP addresses, see Benjamin Edelman, *Web Sites Sharing IP Addresses: Prevalence and Significance*, <http://cyber.law.harvard.edu/people/edelman/ip-sharing/> (last visited Sept. 18, 2005).

130. See *Internet Gambling Funding Prohibition Act: Hearing on H.R. 4419 Before the H. Comm. on Banking and Fin. Servs.*, 106th Cong. 64 (2000) (statement of Gregory A. Baer, Assistant Secretary for Financial Institutions, Department of the Treasury); GAO REPORT, *supra* note 49, at 53 (finding that more than eighty-five percent of Internet gambling websites accept Visa and MasterCard as forms of payment).

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

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

133. See, e.g., Act of Sept. 19, 1890, ch. 908, 26 Stat. 465 (1890) (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); Act of July 27, 1868, ch. 246, 15 Stat. 194, 196 (1868). See generally G. Robert Blakey & Harold A. Kurland, *The Development of the Federal Law of Gambling*, 63 CORNELL L. REV. 923, 931 (1978) (discussing federal attempts to control state lotteries).

134. *People v. World Interactive Gaming Corp.*, 714 N.Y.S.2d 844, 852 (N.Y. Gen. Term

Turning to the specific rules for Internet gambling, currently no state permits Internet-based gambling.<sup>135</sup> Assisting states with that policy choice, the federal Wire Act, which was first enacted in 1961, arguably outlaws Internet gambling,<sup>136</sup> and thus has been the statute of choice in the few federal prosecutions of Internet gam-

---

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 49, 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.

*Id.* Even after *United States v. Lopez*, 514 U.S. 549 (1995), Internet gambling transactions would plainly involve interstate commerce even if the personal computer of the gambler and the server were located in the same state, in part because Internet transmissions between those locations would likely cross state lines and also because of the close relation between those transactions and transactions that plainly cross state lines.

135. See H.R. REP. NO. 108-133, at 5 (2003).

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.

*Id.*

136. See 18 U.S.C. § 1084 (2000). 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.

*Id.*; see also Gottfried, *supra* note 32, ¶¶ 74-81 (discussing the application of the Wire Act to Internet gambling). There is arguably some ambiguity in the text of the Wire Act that may allow Internet gambling business to claim that their businesses are legal. But while the Fifth Circuit has read the Wire Act to outlaw only Internet gambling involving "sporting events or contests," *In re Mastercard Int'l*, 313 F.3d 257, 262 (5th Cir. 2002), the Justice Department has made it clear that it believes the Wire Act more broadly outlaws internet gambling. See Statement of Kevin v. Di Gregory, Deputy Assistant Attorney General, Before the Subcomm. on Crime, Comm. on the Judiciary (June 24, 1998) ("Bets and wagers that would be prohibited under Section 1084 [of the Wire Act] if placed by telephone, are still prohibited even if transmitted via the Internet."), available at <http://www.usdoj.gov/criminal/cybercrime/kvd0698.htm>. Many thanks to Orin Kerr for this point.

bling.<sup>137</sup> But it does so by targeting those directly responsible for the gambling, not the intermediaries who merely facilitate it. Thus, under current law, intermediaries who do not knowingly<sup>138</sup> participate in the gambling activity have no responsibility for it.<sup>139</sup>

### *a. Targeting ISPs*

The first possibility is to use ISPs to limit Internet gambling.<sup>140</sup> As discussed above, the Internet gambling sites tend to be large, stable, and visible operations. And although the source ISPs can be located outside the reach of U.S. officials, destination ISPs<sup>141</sup> must have a presence inside the jurisdiction in which they offer services. Thus, destination ISPs seem to be particularly well suited to assist in limiting U.S. residents' access to gambling websites located abroad. For example, if a destination ISP is aware of particular gambling sites, it should be able to prevent their customers' traffic from reaching those sites. Requiring 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 where the overwhelming majority of transactions are legal.<sup>142</sup> Thus, regulations that burden the site would inflict less collateral damage on innocent users.<sup>143</sup>

137. GAO REPORT, *supra* note 49, at 11 ("To date, the Wire Act is the federal statute that has been used to prosecute federal Internet gambling cases ....").

138. The Wire Act applies only to those who "knowingly" use a wire communication facility to assist gambling. See 18 U.S.C. § 1084 (2000).

139. For a 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).

140. See Jack L. Goldsmith, *What Internet Gambling Legislation Teaches About Internet Regulation*, 32 INT'L LAW. 1115, 1119 (1998).

141. See *supra* Part I.B.2.a.

142. That analysis is open to the strategy that operators of gaming websites might open a wide-ranging "Games Bazaar" involving both legal and illegal activity, the effect of which would be to increase the collateral harm of regulation. The costs imposed by this kind of tactical design, however, should not count as a reason against regulation. And, 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. 189 (2005).

143. Such regulation may nevertheless be costly. On November 24, 2004, the World Trade Organization (WTO) ruled that U.S. laws, such as the Wire Act, violated U.S. commitments to the WTO. Panel Report, *United States—Measures Affecting the Cross-Border Supply of*

At that point, the question becomes one of selecting an appropriate regulatory scheme. Intuitively, this is a case in which a less onerous "hot-list" scheme makes the most sense. First, law enforcement authorities are likely better placed than ISPs to identify illicit gambling sites. Although it is unclear whether ISPs could easily identify the sites as illicit based on the nature of the transmissions going to and from the sites, law enforcement authorities could identify illicit sites—at least the successful ones—for example, by researching with search engines and observing advertisements.<sup>144</sup> Also, because the crime of gambling is victimless in a sense, the object of law enforcement authorities will likely 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 consequently the costs to ISPs' innocent customers.

Nonetheless, significant difficulties exist with this approach, starting with the difficulty of coordinating multistate regulation. Assume, for example, that Nevada wishes to permit certain forms of Internet gambling that Utah prohibits.<sup>145</sup> If Utah required its ISPs to block transmissions to and from the sites in question, Nevada customers would likely be adversely affected. Indeed, this type of problem would be inevitable if an ISP's customer base transcended the state line, absent some technological ability to differentiate among the ISP's customers based on their physical location and to adjust the filter's effectiveness accordingly. Of course, enactment of a single federal regulation would solve much of the problem, largely because of the greater likelihood that all customers of U.S. ISPs would reside in the United States.<sup>146</sup> To be sure, some reason exists to be wary of rapid federalization of

---

*Gambling and Betting Services*, WT/DS285/R at 2.1 (Nov. 10, 2004). A WTO appeals panel later reversed that decision, but did not explicitly endorse federal regulation of Internet gambling under the WTO. See *supra* note 50.

144. The intuition that law enforcement authorities easily could identify the sites if they wished is based in part on the authors' personal observations of the frequency of radio advertising for illegal Internet gambling sites on sports radio stations in some cities.

145. This example is given in Gottfried, *supra* note 32, ¶ 76.

146. The problem is a standard one of regulatory symmetry: in practice, national boundaries tend to bound ISP markets, which often makes imposing regulations at the national level easier. See Mann, *supra* note 51, at 706.



Internet gambling,<sup>147</sup> as a subset of e-commerce, largely because it denies regulators the opportunity to compare the effectiveness of competing approaches.<sup>148</sup>

Another problem is the possibility that such a regulation would violate the First Amendment. As discussed in more detail in the section on child pornography,<sup>149</sup> 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.<sup>150</sup> 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.<sup>151</sup> Thus, the overblocking problem is likely to be less serious in this context.<sup>152</sup> Also of relevance is that the targeted activity—gambling rather than pornography—is entirely commercial, and thus not as likely to garner First Amendment protection. For those reasons, some basis exists for thinking that the schemes this Article proposes would satisfy constitutional scrutiny. Still, to the extent that the

---

147. The problem is complicated by the arguable hypocrisy of state gambling policy, which to an external observer appears 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. This view is further supported by the increasing reliance of state governments on gambling revenue, which surely gives them incentives to combat competition from offshore gambling operations. See Fox Butterfield, *As Gambling Grows, States Depend on Their Cut to Bolster Revenues*, N.Y. TIMES, Mar. 31, 2005, at A24. These inconsistencies in U.S. policy are part of the reason efforts to target overseas gambling operators have been challenged as inconsistent with U.S. obligations under the WTO. *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, *supra* note 143, ¶¶ 3.7-3.9; see also *supra* Part I.B.2.a.

148. 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 that may turn out to be a more effective method for regulating the new industry).

149. See *infra* Part III.A.3.

150. *Ctr. for Democracy & Tech. v. Pappert*, 337 F. Supp. 2d 606, 610-11 (E.D. Pa. 2004).

151. *Contra* Gottfried, *supra* note 32, ¶ 75 (refraining from distinguishing Internet gambling sites from other kinds of websites, eighty-seven percent of which share IP addresses).

152. *Contra id.*

constitutional question remains unclear, it should give regulators some hesitation in pursuing this strategy.<sup>153</sup>

A final concern is that gambling websites would react to ISP blocking by designing their user interfaces to utilize other technologies not susceptible to IP blocking.<sup>154</sup> Any such evolution would likely not place gambling activities outside the reach of ISPs, who would nonetheless be required to carry the communication. Rather, blocking techniques may have to adapt as 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 the program utilizes is one potential response.<sup>155</sup> 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.

The skeptic who doubts Congress's willingness to step into an area traditionally left to state regulation should consider that Congress recently has entertained such legislation: the proposed Internet Gambling Prohibition Act of 2000 would have required ISPs to terminate accounts for those running Internet gambling sites and to block access to foreign Internet gambling websites identified by law enforcement authorities.<sup>156</sup> This Article's analysis

---

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

154. Indeed many gambling websites are beginning to adopt programs that allow gambling without the use of traditional browsers. See, e.g., Starluck Casino, Getting Started, <http://www.starluckcasino.com/slcasino/english/gettingstarted.html> (last visited Sept. 18, 2005).

155. This is a response to the P2P problems suggested by Solum & Chung, *supra* note 39, at 929-30.

156. H.R. REP. NO. 106-655, at 20 (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.

*Id.* For a sympathetic discussion of similar legislation, see Goldsmith, *supra* note 140, at 1117-18.

suggests that such statutes may indeed be an appropriate response for policymakers who view gambling as imposing a serious social harm.<sup>157</sup>

*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, law enforcement authorities apparently could impose a considerable obstacle to the business of those sites by curtailing activity from a small number of intermediaries. Moreover, because this would not involve the potential for overblocking, a First Amendment challenge does not seem plausible. Finally, because a "hot-list" scheme barring transmissions to Internet gambling sites would closely resemble existing "hot-list" schemes with which financial intermediaries already must comply,<sup>158</sup> such a scheme would seem unlikely to impose costs on Internet gambling sites sufficient enough to raise the prospect of worrisome collateral effects on law-abiding customers.

This Article's 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.<sup>159</sup> First, many card issuers voluntarily have limited the use of their credit cards for gambling transactions. In the case of Providian National Bank, the limitation on credit card use seems to have been in response to lawsuits by individuals who refused to pay debts incurred at Internet gambling sites based on the dubious claim that the activity was illegal and that the card issuer so facilitated the activity as to make the debt unenforceable.<sup>160</sup> Other

---

157. See *supra* note 147.

158. See, e.g., OFAC REPORT, *supra* note 100, at 5-43 (describing the regulations requiring financial institutions to block transactions to individuals and countries).

159. See Gottfried, *supra* note 32, ¶ 86; Scott, *supra* note 139, at 490.

160. See Cross-cl., *Providian Nat'l Bank v. Haines* (Cal. Super. Ct. 1998) (No. V980858) (making such a claim); see also Gottfried, *supra* note 32, ¶¶ 82-85; Courtney Macavinta, *Net Gambler Sues Credit Firms*, CNET NEWS, July 24, 1998, <http://news.com.com/2100-1023-213705.html?legacy=cnet&owv>; Courtney Macavinta, *Providian May Bar Customers from Net Gambling*, CNET NEWS, Oct. 22, 1999 (explaining the response by Providian to the *Haines*

issuers seem to have acted out of broader concerns, including concerns about the credit risk involved in gambling transactions.<sup>161</sup> But whatever the reason, those actions apparently have negatively affected the growth of Internet gambling enterprises.<sup>162</sup>

More famously, New York Attorney General Eliot Spitzer has been conspicuously successful in convincing payment intermediaries that facilitating Internet gambling is not in their best interests.<sup>163</sup> Spitzer gained enormous leverage after winning a case in New York that held New York law applicable to Internet gambling regardless of the server's location or the company's registration.<sup>164</sup> Armed with that decision as well as a federal circuit court decision holding that federal law made Internet gambling illegal,<sup>165</sup> Spitzer began negotiating with payment intermediaries to encourage them to limit their involvement with Internet gambling. Presumably, Spitzer was

---

case), <http://news.com.com/2100-1040-231845.html?legacy=cnet>.

161. GAO REPORT, *supra* note 49, 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.

*Id.*

162. Charles Crawford & Melody Wigdahl, *Internet Payment Solutions*, in THE INTERNET GAMBLING REPORT V 88-89 (Mark Balestra ed., 5th ed., Trace Publ'ns 2002) (1997) (estimating that Internet gambling sites that relied on U.S. gamblers saw their revenues decrease by thirty-five to forty percent 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 49, at 4.

[T]he 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.

*Id.*

163. 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. See Gottfried, *supra* note 32, ¶ 86.

164. *People v. World Interactive Gaming Corp.*, 714 N.Y.S.2d 844, 848-50, 858 (N.Y. Gen. Term 1999) (finding the corporation's personal contacts with New York sufficient to exert personal jurisdiction and apply New York state law).

165. *United States v. Cohen*, 260 F.3d 68, 76-77 (2d Cir. 2001).

able, at least implicitly, to threaten litigation against these payment intermediaries as accomplices in the commission of the illegal gambling activity.<sup>166</sup> Regardless of how the pressure was exerted, it was successful. The largest commitment came when Citibank agreed to not approve credit card transactions involving Internet gambling websites.<sup>167</sup> 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.<sup>168</sup> More recently, Spitzer has extended those agreements with commitments from ten additional banks to similarly end approvals for credit card transactions that involve Internet gambling.<sup>169</sup>

Again, as with the activity of ISPs, Congress has considered but not yet enacted legislation targeting payment intermediaries. Specifically, the Unlawful Internet Gambling Funding Prohibition Act<sup>170</sup> would have forbidden payment systems from honoring payments for gambling-related services.<sup>171</sup> The very possibility of such a statute casts a shadow over the negotiations among state regulators and payment intermediaries, thereby making plausible requests for cooperation difficult for the intermediaries to withstand.<sup>172</sup>

---

166. *Contra, e.g., In re MasterCard Int'l Inc.*, 132 F. Supp. 2d 468, 471, 497 (E.D. La. 2001) (holding that a cardmember's use of credit to fund gambling activities at brick-and-mortar establishments does not mean that the credit card company is involved in gambling or the promotion of gambling); *Cie v. Comdata Network*, 275 Ill. App. 3d 759, 760 (1995) (same), *appeal denied*, 662 N.E.2d 423 (Ill. 1996); *Jubelirer v. MasterCard Int'l Inc.*, 68 F. Supp. 2d 1049, 1053 (W.D. Wis. 1999) (same). In the Internet context, however, whether the activity is both illegal and easily identified as illegal is important.

167. Assurance of Discontinuance, In the Matter of Citibank (South Dakota), N.A. (June 21, 2002), <http://www.oag.state.ny.us/Internet/litigation/citibank.pdf>.

168. Assurance of Discontinuance, In the Matter of PayPal, Inc. (Aug. 16, 2002), <http://www.oag.state.ny.us/Internet/litigation/paypal.pdf>.

169. Press Release, Office of New York State Attorney General Eliot Spitzer, Ten Banks End Online Gambling with Credit Cards (Feb. 11, 2003), [http://www.oag.state.ny.us/press/2003/feb/feb11b\\_03.html](http://www.oag.state.ny.us/press/2003/feb/feb11b_03.html).

170. See S. REP. NO. 108-173 (2003) (considering the Unlawful Internet Gambling Funding Prohibition Act, which targeted payment intermediaries); H.R. REP. NO. 108-145 (2003); H.R. REP. NO. 108-133 (2003); H.R. REP. NO. 108-51, pt. 1 (2003); H.R. REP. NO. 107-339, pt. 1 (2001); H.R. REP. NO. 106-771, pt. 1 (2000).

171. See S. REP. NO. 108-173, at 16 (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 32, ¶¶ 87-90.

172. This Article's analysis is limited to the United States. Arthur Cockfield suggests 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, targeting ISPs to limit Internet gambling is not implausible, but regulation of payment intermediaries is likely to be more effective, and less likely to involve collateral effects on lawful transactions and to face complicating legal challenges.

### 3. Child Pornography

Although the First Amendment has limited the ability of the U.S. legal system to condemn pornography broadly, child pornography has long been condemned and made illegal both in the United States<sup>173</sup> and around the world.<sup>174</sup> Specifically, the Sexual Exploitation of Children Act of 1978<sup>175</sup> makes the production or distribution of obscene images of children illegal.<sup>176</sup>

During the 1970s and 1980s, child pornography laws apparently were *relatively* effective, at least in the United States, largely because the distribution of pornography required printed material, which was difficult to find and expensive to purchase if found.<sup>177</sup> But

---

173. *New York v. Ferber*, 458 U.S. 747, 763 (1982) (stating that content which depicts children engaged in sexual conduct is "a category of material outside the protection of the First Amendment").

174. See United Nations Convention on the Rights of the Child, art. 34, Nov. 20, 1989, 28 I.L.M. 1448, 1469 ("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).

175. 18 U.S.C. § 2252A(a) (2000) (outlawing the use of the mail to distribute child pornography or to produce child pornography for distribution through the mail).

176. The law was originally limited to those under age sixteen, but later raised to age eighteen. See Child Protection Act of 1984, ch. 110, § 5, 98 Stat. 204, 205 (1984).

177. See Katherine S. Williams, *Child-Pornography and Regulation of 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: Hearings Before the House Comm. on Gov't Reform*, 108th Cong. (2003) (statement of Linda D. Koontz, Director, Information Management Issues) [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. With the advent of the Internet, however, both the volume and the nature of available child pornography have changed significantly. The rapid expansion of the Internet and its technologies,

with the Internet's advent, the distribution of child pornography has become cheaper and less risky.<sup>178</sup> 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.<sup>179</sup>

This proliferation began on websites, but more recently has shifted primarily to peer-to-peer (P2P) networks, following the same pattern as music piracy.<sup>180</sup> The shift to P2P networks needs to be emphasized 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 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, as no payment may be 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, this Article starts with the possibility of targeting ISPs. 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.<sup>181</sup> That law adopted a "hot-list" regime, under which ISPs are liable if they allow child pornography to be accessed through their services after being notified that the pornography is available at a particular site:

---

the increased availability of broadband Internet services, advances in digital imaging technologies, and the availability of powerful digital graphic programs have led to a proliferation of child pornography on the Internet.

*Id.* at 4.

178. See Williams, *supra* note 177, at 469.

179. In 2002, there were 26,759 reports of child pornography on websites, and 757 reports of child pornography on peer-to-peer networks, a fourfold increase from the previous year). Koontz *Testimony*, *supra* note 177, at 2-3.

180. *Id.* at 6.

181. 18 PA. CONS. STAT. ANN. § 7622 (West 2004).

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.<sup>182</sup>

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.<sup>183</sup> 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, the ability of providers to block access was not as easy as the legislature apparently supposed. The Pennsylvania Attorney General enforced the law against what this Article calls destination ISPs.<sup>184</sup> When the ISPs received notice that child pornography could be accessed over their networks, the ISPs typically attempted to comply by filtering their traffic either for IP addresses, DNS entries, or URLs.<sup>185</sup> In theory at least, any of those approaches might be successful in censoring the targeted content, but each network operates slightly different and was able to implement some of the technologies more efficiently than others.<sup>186</sup> In practice, most ISPs used IP filtering because it was the simplest for them to implement.<sup>187</sup> The problem with IP filtering, however, is that a website can keep the same URL and change IP addresses.<sup>188</sup> Because the URL is the information customers remember to find the

---

182. *Id.*

183. 18 PA. CONS. STAT. ANN. § 7624 (West 2004).

184. *See* Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 620-21 (E.D. Pa. 2004) (explaining that the Attorney General 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).

185. *Id.* at 628.

186. *Id.* at 629.

187. *See id.* at 629, 636-37 (describing specific examples of ISP compliance).

188. *Id.* at 632.



site, monitoring is wholly ineffective if it permits the site to avoid regulation simply by changing the IP address but not the URL. ISPs *could* respond by routinely checking URLs and updating IP addresses.<sup>189</sup> At the time of the *Pappert* litigation, however, the most cost-effective method of monitoring also appeared easy to evade.

Another problem is that IP blocking often leads to blocking content which was not targeted, largely because of "virtual hosting," whereby one web server hosts several websites that share a single IP address but have different URLs.<sup>190</sup> Because of the perception that this so called "overblocking" resulted in blocking protected speech, a district court in 2004 held the statute unconstitutionally overbroad.<sup>191</sup> 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.<sup>192</sup> Additionally, the court was clearly 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 after prohibited material had been removed.<sup>193</sup> Ultimately, the court concluded that these problems left the law beyond the bounds of regulation permitted by the First Amendment.<sup>194</sup> Moreover, the court even went so far as to hold that the statute violated the dormant Commerce Clause.<sup>195</sup> The court generally reasoned that because the statute could be easily evaded, its local benefits were so trivial that the Commerce Clause would not tolerate the inevitable

---

189. *Id.*

190. *Id.* at 617-18, 633.

191. *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 which require ISPs not to provide harmful materials to minors over the Internet. *E.g.*, *PSINet, Inc. v. Chapman*, 362 F.3d 227, 229-30 (4th Cir. 2004); *ACLU v. Johnson*, 194 F.3d 1149, 1152 (10th Cir. 1999); *Am. Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 161, 163-64 (S.D.N.Y. 1997).

192. *Pappert*, 337 F. Supp. 2d at 637-42, 650-51.

193. *Id.* at 642-43. Zittrain, *supra* note 28, provides a thorough discussion of the technological questions involved, detailing a number of steps that ISPs or regulators could take to limit the costs of such regulation.

194. *Pappert*, 337 F. Supp. 2d at 658.

195. *Id.* at 661-63.

burden on other jurisdictions when the blocking affected out-of-state actors.<sup>196</sup>

*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 implausible<sup>197</sup> and because congressional legislation explicitly banning child pornography from the Internet or authorizing states to do so should not be difficult to obtain. The more imposing impediment is how to deal with the First Amendment problem, which is not within Congress' control. A regulator who diligently tried to prevent the blocking of valid speech would perhaps obtain a better result. Still, at least for the time being, 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.<sup>198</sup> The law also apparently would have to provide for notice to blocked URLs and a mechanism for removing a block from URLs once prohibited speech has been removed.<sup>199</sup> In sum, 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 who view child pornography as a highly serious social problem. Again, advances in blocking technology could change that balance in short order. For now, however, even though some states appeared to be unfazed by the *Pappert* decision,<sup>200</sup> the problems with targeting ISPs seem substantial.

### *b. Targeting Payment Intermediaries*

A second option for curtailing child pornography is to target the payment intermediaries who make it profitable for child pornogra-

---

196. *Id.*

197. 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).

198. *Pappert*, 337 F. Supp. 2d at 652.

199. *Id.* at 642.

200. In March 2005, the Utah governor signed a bill very similar to the Pennsylvania statute that was struck down in *Pappert*. Declan McCullagh, *Utah Governor Signs Net-Porn Bill*, CNET NEWS.COM, Mar. 21, 2005, [http://ecoustics-cnet.com.com/Utah+governor+signs+Net-porn+bill/2100-1028\\_3-5629067.html](http://ecoustics-cnet.com.com/Utah+governor+signs+Net-porn+bill/2100-1028_3-5629067.html). The governor's spokesperson indicated that the governor did not "have a concern about the constitutional challenge." *Id.*

phy to be sold over the Internet. As discussed above, a significant amount of pornography is distributed through noncommercial transactions.<sup>201</sup> But commercial websites remain a major source of child pornography on the Internet, providing much of the material that is distributed through noncommercial transactions.<sup>202</sup> Thus, although targeting payment intermediaries would not stop noncommercial distribution of child pornography, it could significantly limit the commercial source of much of the pornography and thus have a substantial effect on the level of wrongful conduct.<sup>203</sup> Indeed, the effectiveness of targeting payment intermediaries might be greater for child pornography sites than 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.<sup>204</sup> Thus, access to credit card processing is essential to the business of commercial pornography websites.<sup>205</sup>

Following a "hot-list" strategy similar to the proposed Unlawful Internet Gambling Funding Prohibition Act,<sup>206</sup> states could pass laws that make it illegal to process credit card transactions from websites offering child pornography. These laws could instruct

---

201. See *Koontz Testimony*, *supra* note 177, at 5 (listing Usenet groups and peer-to-peer networks as principal channels of distribution of child pornography).

202. See *id.* at 5-6. This Article speculates 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.

203. A strategy targeted at limiting commercial exploitation of child pornography could possibly 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.

204. Pornography websites were channeled into the use of credit cards to verify age in part by the affirmative defense offered by section 231 of the Communications Decency Act. 47 U.S.C. § 231(c)(1)(A) (2000) ("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 ....").

205. See *Koontz Testimony*, *supra* note 177, at 5-6 (mentioning a child pornography ring that included websites based in Russia and Indonesia, content malfeasors located out of U.S. reach, and a Texas-based firm that provided credit card billing and access service for the sites).

206. See *supra* note 170 and accompanying text.

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,<sup>207</sup> 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 one could easily predict that federal legislators would be happy to pass, implement, and take credit for any statute that would provide an effective remedy for child pornography. Thus, 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 merchant's ability to outsmart the efforts of intermediaries to suppress such transactions. Intuitively, the intermediaries seemingly could defeat those efforts with relatively little difficulty. First, for transactions to be submitted directly as the transactions of another merchant is a direct violation of Visa and MasterCard rules. Second, with respect to secondary processors, which are permitted to submit transactions for other merchants, Visa and MasterCard already engage in close monitoring that makes it easy to identify transactions from particular illegal sites.<sup>208</sup> 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 maintaining accurate "hot-lists" difficult for law enforcement authorities.<sup>209</sup> The existing tools for monitoring the patterns of merchant transactions, however, including the patterns of chargebacks, which are likely to be high at

---

207. See *supra* text accompanying notes 195-96 (describing the holding of the *Pappert* court on dormant Commerce Clause grounds).

208. We know this from the pleadings in the *Perfect 10* litigation. See *supra* note 78.

209. Although the authors have not engaged in field research to examine the question, the 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. Pornography sites, on the other hand, 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.

sites that provide adult content, would make any sincere<sup>210</sup> 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.<sup>211</sup> Similar procedures for these prohibited payment recipients could be easily plugged into existing structures with little additional cost. 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 an acceptable cost.

In the end, targeting payment intermediaries is unlikely to completely prevent 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 the intermediaries' law-abiding customers. It remains to be seen 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 who view commercial child pornography as an important and serious problem.

#### 4. Internet Piracy

One of the main driving forces behind this Article 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

---

210. 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 providing adult content.

211. See, e.g., OFAC REPORT, *supra* note 100, at 5-43 (describing the regulations requiring financial institutions to block transactions to individuals and countries).

that respond to that problem,<sup>212</sup> this Article addresses the subject only briefly, focusing on the key points of the analytical framework set out above in Part II.<sup>213</sup>

From that perspective, continuing the progression from the sections above, the most salient feature of Internet piracy is the extent to which it has become 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 preventing the posting of copyright-infringing material on static websites through vicarious copyright infringement would be easy, but peer-to-peer networks shield networks from copyright infringement claims through the potential protection afforded by *Sony*.<sup>214</sup> 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.<sup>215</sup>

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.<sup>216</sup> They have thus shielded themselves from the type of vicarious liability found in *Napster*.<sup>217</sup> Moreover, following the lead suggested by Kraakman's analysis of asset insufficiency,<sup>218</sup> networks and ISPs involved in the industry have evolved to become judgment proof,

---

212. Fashioning a regulatory scheme for copyright piracy also must account for the direct effects of the Internet on the nature of the conduct. The Internet's main effect on gambling and pornography has been to facilitate dissemination of activity that remains socially unacceptable. With respect to copyrighted materials, however, the Internet's rise 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.

213. For a recent discussion that focuses directly on the propriety of intermediary liability, see Hamdani, *supra* note 31.

214. See generally *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984) (setting forth the "substantial noninfringing uses" doctrine).

215. See *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1022-24 (9th Cir. 2001).

216. See *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd.*, 380 F.3d 1154, 1163, 1165 (9th Cir. 2004) (refusing to find liability for Grokster even though it aided end users in copyright infringement because the service was fundamentally different than Napster), *vacated*, 125 S. Ct. 2764 (2005).

217. *Id.*

218. See generally Kraakman, *Corporate Liability Strategies*, *supra* note 82, at 868-69 (discussing asset insufficiency as a means to avoid corporate liability and the possible protection afforded by managerial liability).

thereby limiting the effectiveness of sanctions even against the intermediaries. It seems natural to expect that as the technology develops it will be so decentralized as to obviate the existence of any intermediary gatekeeper that could be used to shut down the networks.<sup>219</sup>

Indeed, *despite* the industry's victory in *Napster* and its more recent, albeit limited, victory in *Grokster*,<sup>220</sup> efforts to use intermediaries to limit P2P filesharing have been so ineffective 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.<sup>221</sup> At least initially, the content industry was able to prosecute such claims because peer-to-peer networks and software allowed them to capture enough information about individuals who connect to the network to find the infringers and identify the extent of their infringement.<sup>222</sup> Without this information, copyright protectors would not have enough information to file a claim. Capitalizing on this, new networks and users have taken steps to avoid liability by simply shielding their identities and libraries so that copyright

---

219. See generally Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 685 (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 enforcement claims too harshly. This resonates with the backlash phenomenon described by Mark Roe, *Backlash*, 98 COLUM. L. REV. 217 (1998), and extended in POLITICAL DETERMINANTS OF CORPORATE GOVERNANCE (2003).

220. The industry's victory in *Grokster* does indeed seem to be quite limited as the Supreme Court found the potential for liability not in the substantive copyright violations of the P2P networks' customers, but for the way in which the companies distributed their products. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764, 2770 (2005). The Supreme Court has thus said that future networks can provide identical services so long as they do not actively encourage copyright violations. *Id.* at 2779-83.

221. 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, *Music Pirates: Still on Board*, BUS. WK., Jan. 26, 2004, at 13. In part, this is because the adverse publicity those efforts have generated has 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, Note, *Grossly Excessive Penalties in the Battle Against Illegal File-Sharing: The Troubling Effects of Aggregating Minimum Statutory Damages for Copyright Infringement*, 83 TEX. L. REV. 525 (2004).

222. See Alice Kao, Note, *RIAA v. Verizon: Applying the Subpoena Provision of the DMCA*, 19 BERKELEY TECH. L.J. 405, 408 (2004).

protectors are unable to gather the necessary information to prosecute their claims.<sup>223</sup> And as this evolution of copyright infringement continues, it seems most unlikely that prosecuting individual users will result in an end to the harm.<sup>224</sup>

In the terms of this Article, the most plausible intermediary strategy<sup>225</sup> is regulation of the ISPs that provide 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 to terminate the customer's service. Because such a scheme does not require monitoring by the ISPs but rather relies wholly on monitoring by content providers, it could be implemented with less cost than schemes that would require the ISP to monitor its customers' conduct to identify unlawful filesharing, which strikes us as quite difficult under existing technology and perhaps normatively undesirable in any case.

Interestingly enough, the Digital Millennium Copyright Act already comes close to including such a regime in section 512(a)(6)(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."<sup>226</sup> Why content providers have not relied more heavily on that regime in their efforts to target frequent P2P filesharers is unclear. The best 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.<sup>227</sup>

---

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

224. Perversely, what probably has 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 obtained files. Wendy M. Grossman, *Speed Traps*, INQUIRER (U.K.), Jan. 14, 2005, available at <http://www.theinquirer.net/?article=20718>. Another dissuasion has been the recording industry's systematic effort 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, available at <http://www.pcworld.com/news/article/0,aid,109816,00.asp> (documenting the practice and attributing it to a company called Overpeer, which is apparently an industry anti-piracy company).

225. There are of course other strategies. *E.g.*, *supra* note 57.

226. 17 U.S.C. § 512(a)(6)(i)(1)(A) (2000).

227. Notably, 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 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 57, at 1420-21.



### *B. Breaches of Security*

This Article closes 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 harms are unique to the Internet because they involve conduct that is motivated by the rise of the heavily interconnected networks that comprise the Internet. The harm of these actions is measured by the immense amounts of money spent by end users to purchase software to avoid these problems, the harm to consumers whose personal data is stolen,<sup>228</sup> the time spent repairing damaged computers, and the lost value of computers slowed or rendered inoperable by these incidents.<sup>229</sup> 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 the authors' relative lack of knowledge in the area, the authors are less confident in their ability to discern the relevant policy concerns in these areas than for the content harms discussed above. This Article discusses the topic generally only to illustrate two obvious points that this Article's framework suggests for these issues.

#### *1. Lack of Strong Intermediaries*

In comparison to the dissemination of illegal content that was the subject of the preceding sections, this is not an area where a need for legislative intervention to sanction intermediaries is nearly so obvious. As the above examples 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

---

228. Of course, some data theft does not involve the Internet. However, the Internet certainly exacerbates the data security problems our society confronts.

229. One estimate put the total cost of viruses at \$55 billion for 2003. See *Compressed Data*, *supra* note 15. Significant evidence exists to suggest that these problems are increasing. According to a recent study, for example, the total number of phishing scams in December 2004 was 9,019, an 8,000% increase over the 107 such scams in December 2003. Brian Krebs, *Tech Heavyweights Agree to Share 'Phishing' Data*, WASHINGTONPOST.COM, Feb. 14, 2005, <http://www.washingtonpost.com/wp-dyn/articles/A24065-2005Feb14.html>. See also *Internet 'Phishing' Scams Soared in April*, WALL ST. J., May 24, 2004, at B5 (reporting that phishing scams more than doubled between March and April 2004).

readily identifiable intermediaries exist that can readily control the conduct yet choose not to do so. In some cases, direct regulation seems both inevitable and potentially effective. For example, the rash of recent data make it likely that Congress will enact legislation that regulates the activities of those that handle data. In contexts in which that kind of regulation can be made effective<sup>230</sup>—and the large size of many of the major data warehouses makes that seem a plausible solution to the problem of data security—then there is considerably less need to rely on intermediaries.

The context of security harms differs in two obvious respects from that paradigm. First, whether any intermediary can readily control the conduct in question is not clear. 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 possible to view the software designer as yet another intermediary that could solve harms from viruses, spam, and hacking, it is less useful to think of that as intermediary liability than as a rapidly developing species of products liability.<sup>231</sup>

Looking solely at the intermediaries identified in Part I.B.2 of this Article, it seems unlikely that ISPs serving those who introduce viruses and spam into the Internet community can control the misconduct because of the difficulty of identifying the transmissions that cause the problem and of filtering out the malicious code.<sup>232</sup>

---

230. Businesses that handle data have exposure to third parties under civil liability regimes. In addition, the FTC and some states have been active in pursuing businesses that inaccurately portray their privacy policies. *See, e.g.,* Jonathan Krim, *Credit Report Firm Settles FTC Charges*, N.Y. TIMES, Aug. 16, 2005, at D1 (discussing a settlement over charges that the company deceived customers seeking free credit reports). Yet the magnitude of recent security breaches suggests that those solutions are likely to be insufficient. *See, e.g.,* Eric Dash & Tom Zeller, Jr., *Mastercard Says 40 Million Files Are Put at Risk*, N.Y. TIMES, June 18, 2005, at A1.

231. For a fine note outlining the perverse market incentives that have led to a market failure for secure software, see Douglas A. Barnes, Note, *Deworming the Internet*, 83 TEX. L. REV. 279 (2004).

232. 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 generally* LICHTMAN & POSNER, *supra* note 30, at 5 (arguing for liability that forces such cooperation). But this Article's 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 this Article suggests to combat the harms discussed in this Part involve intermediaries who have the ability to prevent harm in the first instance. For a discussion of the rapidly evolving technological possibilities, see Zittrain, *supra* note 28, at 91-105.

Similarly, whether ISPs serving the customers victimized by security breaches can solve the problem is unclear, again because of the difficulty they face in designing reliable systems for identifying harmful traffic. 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 hosted on computers located outside U.S. jurisdictions is an empirical question to which the authors do not know the answer. But even if it turns out that those ISPs are located within the United States, targeting them will simply force those behind phishing scams to move their operations abroad.<sup>233</sup> This does not mean that devising effective intermediary-based strategies is impossible. It is, however, likely to require a remedy that is categorically more disruptive of the Internet's physical and social character than the remedies discussed above.<sup>234</sup>

## *2. Market Incentives Already Exist*

At the same time, market incentives appear to be driving intermediaries to 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.<sup>235</sup> 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 unsure 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

---

233. Websites that host some phishing 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.

234. Zittrain, *supra* note 28, at 105-13 (emphasizing the potential for highly intrusive yet effective actions in this area).

235. Compare, e.g., Yahoo Mail's touting of its spam filters, Yahoo! Mail ("Powerful spam protection: Read only the mail you really want"), <http://mail.yahoo.com/?intl=us> (last visited Apr. 8, 2005), with Earthlink's spamBlocker software, provided free of charge to Earthlink customers, Earthlink ("Powerful Junk Email Protection! We can help. Our spamBlocker tool eliminates virtually 100% of junk email."), <http://www.earthlink.net/software/free/spamblocker/> (last visited Apr. 20, 2005).

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.<sup>236</sup> Further, phishing scams have provided motivation for new technologies and new firms to spring up to combat the danger.<sup>237</sup> 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.

In the context of data security, we also see promising responses from intermediaries. For example, the credit card networks have moved promptly to terminate their relationships with CardSystems Solutions after CardSystems was the victim of a large data theft, relying in part on the failure of CardSystems to comply with network standards for data protection.<sup>238</sup> To be sure, we do not know that the networks would have acted without the public outcry that accompanied this incident.<sup>239</sup> Nevertheless, the rapid response does underscore the distinction between data security and gambling. Visa, MasterCard, and American Express gain nothing from insecure data protection by their members and related processors. This is quite different from the gambling context, where the networks have the profits from the underlying transactions to offset against the costs of allowing the merchants to remain in the network.

This point should not be pushed too far. Doug Lichtman and Eric Posner, for example, have argued with some force that the market forces discussed here are suboptimal, so that the efforts this Article identifies remain insufficiently vigorous.<sup>240</sup> To the extent those responses are suboptimal, the case for intermediary liability is

---

236. See, e.g., Krebs, *supra* note 229 (noting that Microsoft, eBay, and Visa recently signed agreements to work with a firm that gathers information on phishing incidents).

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

238. See, e.g., Todd R. Weiss, *Visa, Amex Cut Ties With CardSystems Due to Breach*, COMPUTERWORLD, July 25, 2005, at 10.

239. See Jonathan Krim, *Credit Data Firm Might Close: After Databases Hacked, Customers Cancel Contracts*, WASH. POST, July 22, 2005, at D2 (discussing congressional hearings on proposed data protection legislation after CardSystems data breach).

240. See LICHTMAN & POSNER, *supra* note 30, at 26-27.

stronger, as they recognize.<sup>241</sup> This Article's 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. ISPs' efforts to date certainly have not put them in a position to prevent this misconduct entirely, but they do reflect at a minimum an effort to eradicate the conduct, which differs substantially from the response the typical ISP takes to respond to the possibility that its customers might be purchasing child pornography or gambling online. If market incentives are truly 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.

### CONCLUSION

The Internet is coming of age. Though at the Internet's advent 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. Virtually every U.S. company of any significant size, even those whose core business is entirely unrelated to the Internet, has incorporated the Internet into its business model 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 Internet users.

As the Internet enters the final stage in its development, this Article suggests that lawmakers carefully reconsider the early policy of Congress that Internet intermediaries should not bear any burden in bringing order to the Internet. This policy ignores an essential truth of the online world, namely that anonymity and porous international borders make targeting primary malfeasors difficult, if not impossible. Internet intermediaries, on the other

---

241. *See id.*

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 technological 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 necessary.

The Internet is indeed at a crossroads in its development. Whether pirates will continue to threaten legitimate users of the Internet or instead 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, for example, payment intermediaries with respect to child pornography, may resist reforms vigorously. Conversely, 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 this Article addresses. This Article has no firm conviction about the shape of the final outcome but is offered in the hope that it can aid the design of sensible Internet regulation.