Cornell Law Review

Volume 87
Issue 4 *May 2002*

Article 1

Who's Liable for Cyberwrongs

Assaf Hamdani

WHO'S LIABLE FOR CYBERWRONGS?

Assaf Hamdani†

The Internet has provided new opportunities for wrongdoers and novel challenges for law enforcement. Frustrated by the relative anonymity of users, plaintiffs and law enforcers have increasingly sought to hold Internet Service Providers (ISPs) liable for their users' misconduct. Yet, legal analysis of ISP liability is balkanized, confining itself to particular doctrinal contexts, thus obscuring common issues underlying all instances of ISP liability. This Article rectifies this shortcoming by developing a new framework for evaluating ISP liability: the incentive-divergence thesis. Because the incentives of ISPs diverge from those of their users, subjecting ISPs to full liability would produce excessive censorship of Internet communication. Legal responses to this risk of excessive censorship should therefore be tailored to the market's ability to align ISPs' incentives with those of their users. The Article proposes three distinct strategies for imposing ISP liability: combining strict ISP liability with scaled-down penalties, regulating the ISP-subscriber interface, and imposing negligence-based liability. The Article also illuminates several existing legal puzzles: the peculiar doctrine of vicarious infringement and its application in the Napster *case, the regulation of ISP liability under the new Digital Millennium Copyright Act, and the optimal liability regime for illegal sales on auction sites.*

† S.J.D. candidate and John M. Olin Fellow in Law and Economics, Harvard Law School. This Article greatly benefited from comments and criticism by Lucian Bebchuk, Avi Bell, Reinier Kraakman, Dan Markel, Gideon Parchomovsky, Steve Shavell, and workshop participants at the Berkman Center for Internet and Society, Harvard Law School. Financial support was provided by the John M. Olin Center for Law, Economics, and Business at Harvard Law School.

INTRODUCTION

Like the new frontier of the Wild West in the nineteenth century, the booms and busts of the Internet have been accompanied by new opportunities for criminals and new challenges for law enforcement. The global reach of the Internet, its inexpensive transmission of information, and the relative anonymity of its users all contribute to the treacherous environment for law enforcement.[1] However, unlike the Wild West, most people's access to the Internet comes through a select group of gatekeepers known as Internet Service Providers, or ISPs.[2]

---

1 *See, e.g.*, PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, U.S. DEP'T OF JUSTICE, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET (2000), http://www.usdoj.gov/criminal/cybercrime/unlawful.htm (last visited Jan. 19, 2002).

2 ISPs provide users with various Internet-related services. Common examples of ISPs include: Internet access providers (companies that enable their subscribers to access the Internet), web-hosting service providers (companies that host their suhscribers' web pages on their servers and enable third parties to access these pages), and online service providers (companies that operate a website and enable third parties to post materials on

Unlike their users, ISP gatekeepers are readily identifiable and susceptible to sanction. These dual characteristics have led to a consensus that, under appropriate circumstances, ISPs should be held legally liable for their users' wrongdoing.[3] ISP liability, however, presents lawmakers, courts, and academics with a host of new dilemmas, including the following: (1) To what extent should an ISP be liable when it enables its customers to swap unauthorized digital copies of copyrighted music?; (2) Should an ISP be liable for hate material offered for sale through its auction site?; and (3) Under what conditions should a website offering its users the ability to upload materials to its "forums" sections be responsible when its users post defamatory statements?

Oddly, the literature so far has addressed each issue separately, confining itself to the particular doctrinal question at stake.[4] Commentators have debated, for example, whether ISPs should face direct, vicarious, or contributory liability for copyright infringement by users,[5] and whether ISPs should be deemed publishers, distributors, or common carriers in determining their liability for online defamation.[6] Unfortunately, this fragmented approach obscures the common fundamental features that underlie all instances of ISP liability. All cases of ISP liability require courts and legislators to delineate the appropriate scope of the liability imposed on a third party—the ISP—for the misconduct of its users. In all cases, the ISP has exclusive technical control over user misconduct, and is thus positioned to prevent misconduct—by blocking user access to the Internet, for example—without the cooperation of the user. Relatedly, the key issue in all

---

their site). Unless stated otherwise, I will use the term ISP to denote all three. For an example of a statutory definition of ISP, see *infra* note 166.

3 To be sure, and as will be demonstrated throughout the Article, much controversy exists over the desirable *scope* of ISP liability. Nonetheless, the basic principle that ISPs might, under appropriate circumstances, face liability for their subscribers' misconduct is undisputed. *See generally* TIMOTHY D. CASEY, ISP LIABILITY SURVIVAL GUIDE (2000) (providing guidance to ISPs on avoiding liability for subscriber misconduct).

4 One notable exception is Professor Katyal's recent article on law enforcement in cyberspace. *See* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003 (2001) (developing strategies for dealing with a wide range of cybercrimes). While his article explores various strategies of law enforcement in some depth, it provides a relatively brief analysis of the important topic underlying this Article—designing optimal liability standards for ISPs. *See id.* at 1095–1101.

5 For a discussion of the controversy over the liability of ISPs for subscriber infringement, see *infra* Part IV.A.

6 *See generally* Jonathan A. Friedman & Francis M. Buono, *Limiting Tort Liability for Online Third-Party Content Under Section 230 of the Communications Act*, 52 FED. COMM. L.J. 647, 664–65 (2000) (arguing against the imposition of distributor liability on service providers); David R. Sheridan, Zeran v. AOL *and the Effect of Section 230 of the Communications Decency Act upon Liability for Defamation on the Internet*, 61 ALB. L. REV. 147, 179 (1997) (arguing that service providers should face "distributor liability" for defamation); *Developments in the Law—The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1612–22 (1999) (describing the debate over the proper classification of ISPs).

these cases is not the technical ability to prevent misconduct, but the extent to which ISPs can distinguish legitimate and illegitimate user activities. Transcending doctrinal boundaries, these common yet unnoticed features call for the development of a general framework for analyzing and designing ISP liability.

This Article adds four key insights to the analysis of ISP liability.[7] First, the Article identifies ISP liability as a coherent analytical category of liability, and locates it within the larger framework of third-party liability.[8] Second, the Article explains why strict liability—the traditional prescription of economic analysts for the liability of primary wrongdoers—will produce overdeterrence when applied to liable third parties such as ISPs. Third, the Article shows that no single rule should cover all cases of third-party liability—an observation that I label the "incentive-divergence thesis." Thus, the Article provides a novel framework capable of tailoring legal regimes to different types of Internet services. Specifically, I offer three distinct strategies for implementing the incentive-divergence thesis in setting ISP liability: strict ISP liability with scaled-down penalties, regulation of the ISP-subscriber interface, and negligence-based liability. Fourth, and finally, the Article demonstrates the illuminating power of the incentive-divergence thesis by using it to explain otherwise mysterious aspects of the recent *Napster* decision[9] and Title II of the Digital Millennium Copyright Act of 1998.[10]

The implications of my analysis can be seen in contrast to the standard law-and-economics position calling for strict liability. The standard of strict liability is generally preferred, because it not only provides defendants with optimal incentives to prevent misconduct, but also ensures that defendants will adopt an optimal level of activity.[11] Under this conventional position, ISPs would face strict liability for user misconduct. Consider the liability of an Internet access provider, such as Yale University, for copyright infringement by students

---

7 This Article does not consider the fundamental question whether the Internet could be governed by traditional legal regimes. For representative examples of this debate, see David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1400–02 (1996) (expressing skepticism over the feasibility of traditional legal regulation in cyberspace); and Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1199–1201 (1998) (criticizing the position adopted by Johnson and Post).

8 For a review of the existing scholarship on third-party liability, see *infra* Part I.A. The term "third party" is often used to distinguish third parties from primary wrongdoers and victims (second parties). *See also* Katyal, *supra* note 4, at 1007–08 (referring to ISPs as "third parties" and victims as "second parties").

9 A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), *aff'g in part and rev'g in part* 114 F. Supp. 2d 896 (N.D. Cal. 2000).

10 17 U.S.C. § 512 (Supp. V 1999).

11 *See, e.g.*, WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW 66–71 (1987); Steven Shavell, *Strict Liability Versus Negligence*, 9 J. LEGAL STUD. 1, 2–3 (1980).

who use Napster while using private computers connected to the Yale network.[12] If Yale were to face strict liability, the argument goes, it would exercise the socially desirable level of effort to prevent copyright infringement by its users, and price its Internet services appropriately.

Notably, strict liability appeals not only to economic theorists; beginning with the endorsement of strict liability by President Clinton's Information Infrastructure Task Force on the Protection of Intellectual Property over the Internet,[13] a substantial number of courts, including the Northern District of California in the *Napster* case,[14] and academics have urged applying strict liability to ISPs.[15]

This Article shows otherwise. I argue that holding ISPs strictly liable for the full social harm produced by user misconduct would induce them to adopt excessive levels of monitoring and employ overly zealous censorship policies. This is because one of the key assumptions of the economic literature, namely, that actors capture the full value of their conduct, does not necessarily apply to ISPs, or, indeed, to any third parties. While Yale might be technically positioned to control the transmission of information through its networks—by blocking access to Napster, for example—Yale does not capture the

---

12 This example is not imaginary. Indeed, in April 2000, the rock group Metallica sued Yale University as the provider of Internet access to its students using Napster's services. *See* John Borland, *Yale Drops Napster After Legal Pressure*, CNET NEWS.COM, Apr. 19, 2000, *at* http://news.cnet.com/news/0-1005-200-1719530.html. Immediately afterwards, Yale decided to block its students' access to Napster. *Id.*

13 *See* RONALD H. BROWN & BRUCE A. LEHMAN, INFO. INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 114–24 (1995) (describing the development of the need for strict liability to ISPs for subscriber copyright infringement), *available at* http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf.

14 *See Napster, Inc.*, 114 F. Supp. 2d at 913–22, 927 (granting preliminary injunction against Napster after finding it strictly liable for all copyrighted files downloaded through its server); Playboy Enters. v. Frena, 839 F. Supp. 1552, 1554–59 (M.D. Fla. 1993) (holding the operator of a bulletin board service that allowed users to upload illegal copies of Playboy photographs liable for copyright infringement, regardless of prior awareness), *superseded by statute as stated in* ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619 (4th Cir. 2001); Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, at *4–*5 (N.Y. Sup. Ct. May 24, 1995) (finding that Prodigy, an ISP, is a "publisher" for defamation purposes and thus should be held strictly liable for defamatory statements posted on its bulletin boards), *superseded by statute as stated in* Zeran v. American Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) (explaining that 47 U.S.C. § 230 "forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions"); *see also* Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1852, 1856 (2000) (emphasizing that the risk of courts' holding ISPs strictly liable is real).

15 *See* Jane C. Ginsburg, *Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace*, 95 COLUM. L. REV. 1466, 1493–94 (1995) (describing policy considerations behind imposing vicarious liability for copyright infringement on commercial ISPs); I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 1044 (1994) (arguing that imposing strict liability on ISPs will make them internalize the social costs of wrongdoing and adjust the scope of their activity accordingly).

full value of such information. Rather, student users of Napster are the primary beneficiaries of information transmitted through Yale's network. Stated differently, Yale does not bear the full cost of its policing effort; the cost is, at least in part, borne by Napster users attending Yale. Hence, under a regime of strict liability for user misconduct, Yale would assign disproportionate weight to the risk of legal liability and disregard the loss caused to students as a result of the newly blocked or removed user information. This divergence of incentives would lead Yale to monitor user information excessively, and remove materials suspected of being unlawful, even when social interest dictates otherwise.

Having identified the potential for overdeterrence, I proceed to develop the incentive-divergence thesis by crafting a framework for optimizing liability standards for ISPs. My analysis proceeds in three stages.

First, I identify two existing approaches concerning the appropriate response to overdeterrence produced by the divergence of user and ISP incentives. These two analyses may be labeled the "restrictive" and "market" approaches. Noting the divergence of incentives between primary wrongdoers and ISPs, the restrictive approach calls for placing categorical limitations on third-party liability.[16] By contrast, the market approach dismisses the risk of ISP overdeterrence on the grounds that competition among ISPs would eliminate the divergence of incentives between users and service providers.[17]

In the second stage, I demonstrate the shortcomings of both existing approaches and offer a new alternative: the incentive-divergence thesis. My analysis focuses on contractual failures that produce divergent incentives, on the one hand, and market forces that alleviate the effects of such divergent incentives, on the other. I argue that the severity of overdeterrence varies across markets and contractual relationships, and that the law should take these differences into consideration. In an ideal world, the market approach would be correct, and ISPs and subscribers would contract to avoid excessive monitoring by ISPs. In the real world, however, transaction costs preclude such

---

16 Most calls for placing categorical limitations on third-party liability have arisen in the analogous context of employer vicarious liability for hostile environment based on coworker harassing speech, an area where the imposition of liability has sparked much debate. *See, e.g.*, Kingsley R. Browne, *Workplace Censorship: A Response to Professor Sangree*, 47 RUTGERS L. REV. 579, 582–85 (1995) (positing that the vicarious liability of employers induces them to over-censor employee speech); Eugene Volokh, *What Speech Does "Hostile Work Environment" Harassment Law Restrict?*, 85 GEO. L.J. 627, 647–48 (1997) (arguing that cautious employers would excessively restrict employee speech). *But see* Suzanne Sangree, *Title VII Prohibitions Against Hostile Environment Sexual Harassment and the First Amendment: No Collision in Sight*, 47 RUTGERS L. REV. 461, 479 (1995) (suggesting that "employee morale" would prevent overregulation of speech by employers).

17 *See* discussion *infra* Part II.B.2.

an ideal solution, and ISPs and subscribers thus maintain divergent incentives. Moreover, the magnitude of this divergence of incentives depends on factors such as the degree of competition in the relevant market, the existence of profit-sharing agreements between the parties, and the cost of ex post negotiation. For example, auction sites, whose fees increase in proportion to the sale price of items sold through their site, have monitoring incentives closely aligned to those of their subscribers. By contrast, universities, which provide free Internet access to their students, are subject to very different incentives than their users.

Thus, in the third stage, I use the incentive-divergence thesis to tailor three specific strategies for optimizing deterrence notwithstanding divergent incentives. The first legal strategy, which I call scaled-down strict liability, would impose strict liability on ISPs while reducing the magnitude of penalties. This simple strategy, although intuitively appealing to the economic mind, would result in optimal deterrence only in a very limited set of cases. Specifically, scaling down penalties under a strict liability regime would achieve optimal deterrence only for ISPs that, at the margin, suffer an actual loss for each item screened off their system. ISPs will suffer such a loss for each item removed from their systems only if their contract with their subscribers provides for a profit-sharing agreement, as in the case of auction sites.[18]

The second strategy, which I label interface regulation, seeks to regulate the ISP-subscriber interface. Under this strategy, lawmakers will seek to regulate the relationship between ISPs and their subscribers with the aim of assisting the parties to overcome their divergence of incentives through private contracting.

The third strategy aims to render the divergence of incentives irrelevant by making the state, rather than ISPs, set the desirable level of monitoring. This goal can be achieved through either a monitoring-regulation regime or a negligence-based regime. A monitoring-regulation regime assigns lawmakers the task of specifying the extent to which ISPs should inspect the information disseminated through their networks. Monitoring regulation differs from interface regulation in that it does not touch most of the contractual arrangements between ISP and subscriber, focusing instead on the narrow question of monitoring. Like monitoring regulation, properly designed negligence standards might also achieve the right level of monitoring by ISPs. The key difference between the negligence-based regime and the monitoring-regulation regime lies in the identity of the institution

---

18 *But see* Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1094 (C.D. Cal. 2001) (holding that an auction site is not liable for infringing items posted for sale on its site). For a detailed analysis of the optimal legal regime for auction sites, see *infra* Part IV.C.

setting the optimal level of monitoring. Under negligence, courts will set the optimal level of monitoring that ISPs must adopt. In contrast, under a monitoring-regulation regime, a regulator will set the desirable level of monitoring. As I will explain below,[19] these mechanisms thus differ with respect to their suitability to the rapid technological changes characterizing cyberspace.

I illustrate the insights produced by the incentive-divergence thesis by exploring three aspects of ISP liability. First, I analyze the puzzling doctrine of vicarious liability for copyright infringement, most recently applied in the *Napster* cases.[20] The incentive-divergence thesis, I argue, supplies a novel understanding of the economic function of vicarious liability, and sheds a new light on the *Napster* decision. Second, I evaluate the regulatory framework adopted by Congress in Title II of the Digital Millennium Copyright Act of 1998.[21] This Act mildly alleviates the divergence of incentives between subscribers and ISPs. I argue, however, that these measures are insufficient, and fail to assign the proper weight to the different incentives of providers of hosting services and the providers of Internet access. Finally, I devise a regime to govern the liability of auction sites, such as eBay, for unlawful items offered for sale through their system.

The implications of the incentive-divergence thesis go beyond cyberspace. Legal systems increasingly rely on complex regimes of third-party liability. Prominent examples include accomplice liability in criminal law; lender liability for cleanup costs; and underwriter, lawyer, and accountant liability for securities fraud.[22] But while the practical role of third-party liability is gaining in importance, the optimal structure of third-party liability has received scant attention by the academic literature.[23] This Article advances the understanding of

---

19 *See infra* Part III.C.3.

20 A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), *aff'g in part and rev'g in part* 114 F. Supp. 2d 896 (N.D. Cal. 2000).

21 17 U.S.C. § 512 (Supp. V 1999).

22 *See generally* Sanford H. Kadish, *Complicity, Cause and Blame: A Study in the Interpretation of Doctrine*, 73 CAL. L. REV. 323 (1985) (analyzing accomplice liability in criminal law); Lewis D. Lowenfels & Alan R. Bromberg, *Liabilities of Lawyers and Accountants Under Rule 10b-5*, 53 BUS. LAW. 1157 (1998) (reviewing recent development in secondary liability for securities fraud); Michael I. Greenberg & David M. Shaw, Note, *To Lend or Not to Lend—That Should Not Be the Question: The Uncertainties of Lender Liability Under CERCLA*, 41 DUKE L.J. 1211 (1992) (reviewing lender liability under U.S. environmental law). *See also* David B. Wilkins, *Making Context Count: Regulating Lawyers After* Kaye, Scholer, 66 S. CAL. L. REV. 1145, 1160–1215 (1993) (discussing attorney liability in the aftermath of the savings and loan crisis).

23 In his authoritative book providing a comprehensive analysis of the economic theory of liability, Professor Steven Shavell only tangentially addresses the theory of third-party liability by discussing the related topic of vicarious liability. *See* STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW 170–75 (1987); *see also* A. Mitchell Polinsky & Steven Shavell, *The Economic Theory of Public Enforcement of Law*, 38 J. ECON. LITERATURE 45 (2000) (offering a review of the economic theory of public enforcement, but providing no discussion of

third-party liability by systematically analyzing one subset of third-party liability cases—those in which the third party has full technical control over the primary wrongdoer's conduct. Instances of this type of third-party liability include employer liability for employee communications under sexual harassment law,[24] liability of distributors of obscene films,[25] and liability of third parties for defaming statements.[26] In all these cases, the divergence of incentives between the third party and the primary wrongdoer might lead the third party to be too cautious. Accordingly, the incentive-divergence thesis, and the legal strategies I develop under that thesis, could be useful in eliminating overdeterrence in these cases as well.

The Article is organized as follows. Part I lays the groundwork for analyzing ISP liability by outlining existing economic theories of primary and third-party liability. This Part highlights the prominent role of strict liability within the economic literature, reviews the existing economic understanding of third-party liability, and introduces the overdeterrence phenomenon associated with ISP liability. Part II outlines the incentive-divergence thesis, and compares it to the market approach and the restrictive approach. This Part identifies the transaction costs that produce overdeterrence and explores the role of market forces in limiting the severity of the problem. Part III introduces three strategies for implementing the incentive-divergence thesis. These strategies include scaled-down strict liability, interface regulation, and negligence-based liability. Part IV illustrates the wider implications of the incentive-divergence thesis by analyzing ISP vicarious liability for copyright infringement, the Digital Millennium Copyright Act, and the liability of auction sites for illegal items posted for sale on their system.

I
ISP LIABILITY AND OVERDETERRENCE

This Article contends that strict liability, although correctly embraced by the economic literature as the optimal standard of liability

---

third-party liability). By contrast, the economic literature studying the liability of lenders for cleanup costs has extensively examined third-party liability. *See, e.g.*, Marcel Boyer & Jean-Jacques Laffont, *Environmental Risks and Bank Liability*, 41 EUR. ECON. REV. 1427 (1997); Rohan Pitchford, *How Liable Should a Lender Be? The Case of Judgment-Proof Firms and Environmental Risk*, 85 AM. ECON. REV. 1171 (1995); Kathleen Segerson, *Liability Transfers: An Economic Assessment of Buyer and Lender Liability*, 25 J. ENVTL. ECON. MGMT. S-46 (1993).

24 *See supra* note 16.

25 *See, e.g.*, United States v. X-Citement Video, Inc., 513 U.S. 64, 67–78 (1994) (interpreting the relevant statute to require knowledge of minority status by child pornography distributor in order to avoid constitutional challenges).

26 On the three-tiered regime of liability for defamation, see Barry J. Waldman, *A Unified Approach to Cyber-Libel: Defamation on the Internet, A Suggested Approach*, 6 RICH. J.L. & TECH. 9, ¶ 33 (Fall 1999), *at* http://www.richmond.edu/JOLT/v6i2/note1.html.

for primary wrongdoers, should not govern ISP liability for subscriber misconduct. As necessary background for the Article's thesis, this Part first outlines the current economic theory of third-party liability. Then, after discussing the prominent role of strict liability in the economic literature, I show that, given the different incentive structure facing primary wrongdoers and third parties, imposing strict liability on ISPs would result in overdeterrence—excessive monitoring and overzealous censorship by ISPs.

A. The (Missing) Theory of Third-Party Liability

Relying on the general framework developed by Reinier Kraakman,[27] this subpart outlines the basic theory of third-party liability and its implications for ISP liability. I focus on three aspects of the theory: why third parties are held liable, why ISPs are targeted, and the nature of the distinction between primary and third-party liability.

1. *Why ISP Liability?*

Deterrence theory seeks to impose on wrongdoers the social cost of their wrongdoing.[28] In our context, this would mean making subscribers—such as Yale students who use Napster—liable for the full cost of their misconduct. The conditions of the Internet environment, however, might make this goal unattainable. Consider the challenge of imposing sanctions on subscribers who use the Internet to violate copyright laws. The relative anonymity of Internet users makes detection of those who violate copyright laws very costly; absent Yale's cooperation, record companies will not easily be able to identify student users of Napster.[29] Even when the identity of infringers is uncovered, they often turn out to be judgment-proof teenagers or college

---

27 *See* Reinier Kraakman, *Gatekeepers: The Anatomy of a Third Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53 (1986). Several writers have analyzed a related topic: the allocation of liability between corporations and their employees. *See, e.g.*, Steven P. Croley, *Vicarious Liability in Tort: On the Sources and Limits of Employee Reasonableness*, 69 S. CAL. L. REV. 1705 (1996) (arguing that corporate, rather than personal, liability best promotes reasonable decisionmaking); Harry A. Newman & David W. Wright, *Strict Liability in a Principal-Agent Model*, 10 INT'L REV. L. & ECON. 219, 220 (1990) (finding that "strict liability induces the owner to offer employment contracts that motivate the agent to take a socially optimal level of care"); Alan O. Sykes, *The Economics of Vicarious Liability*, 93 YALE L.J. 1231 (1984) (using economic analysis to evaluate the efficiencies of vicarious liability).

28 *See infra* Part I.B.

29 *See, e.g.*, Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1206–08 (2000) (describing the cost of detecting, prosecuting, and punishing infringers). Of course, the cost of detecting Internet users is determined by the relevant legal regime and the architecture of the Internet, which in turn is also affected by regulation. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (analyzing the interaction of these elements).

students, who lack the means to pay damages.[30] Thus, in many cases it would be impossible to impose upon copyright-infringing Internet users the full optimal penalties dictated by deterrence considerations. Expanding liability to third parties is thus required to cope with the underdeterrence of Internet subscribers.[31]

In the case of cyber-misconduct, potential candidates for third-party liability include, among others, makers of personal computers, developers of Internet browsers, and makers of modems.[32] Liability should be expanded, however, only to those parties positioned to prevent misconduct at a reasonably low cost.[33] Following doctrine and academic literature, this Article takes ISP liability as a given, and assumes that ISP liability is justified due to the ability of Internet service providers to prevent subscriber misconduct cheaply.

Granted the expansion of liability to ISPs, the Article will focus on the nature of the liability standards that should govern ISP liability. The literature dealing with third-party liability has struggled mostly with the basic need for third-party liability in particular contexts.[34] But the challenge posed by enlisting ISPs to prevent user misconduct is clearly different. The failure of subscriber-only liability to prevent cyber-misconduct is virtually undisputable, and there is a general consensus that ISPs should be harnessed to the preventive effort. At the same time, however, there is a controversy over identifying the standard that should govern ISP liability for user misconduct. This aspect of third-party liability, which has remained curiously unexplored by the economic literature, is the focus of this Article.

---

30 *See, e.g.*, Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards a Coherent Theory for Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring over the Internet*, 18 HASTINGS COMM. & ENT. L.J. 729, 734–35 (1996) (pointing out that many of the most notorious Internet criminal prosecutions brougbt by the government have targeted college students); Michael B. Rutner, Note, *The ASCAP Licensing Model and the Internet: A Potential Solution to High-Tech Copyright Infringement*, 39 B.C. L. REV. 1061, 1070 (noting that most cyber-infringers are individuals who "do not have enough assets to make legal action worthwhile").

31 *See* Reinier H. Kraakman, *Corporate Liability Strategies and the Costs of Legal Controls*, 93 YALE L.J. 857, 888–96 (1984) (explaining that third-party liability is required to address "enforcement failures" leading to underdeterrence).

32 *See* Yen, *supra* note 14, at 1864 (noting that, in theory, all providers of information technology could be held liable).

33 *See* Howell E. Jackson, *Reflections on* Kaye, Scholer*: Enlisting Lawyers to Improve the Regulation of Financial Institutions*, 66 S. CAL. L. REV. 1019, 1040–41 (1993); Kraakman, *supra* note 31, at 61.

34 *See generally* Stephen Choi, *Market Lessons for Gatekeepers*, 92 NW. U. L. REV. 916 (1998) (providing a thorough analysis of the justification for imposing liability on financial intermediaries); Victor P. Goldberg, *Accountable Accountants: Is Third-Party Liability Necessary?*, 17 J. LEGAL STUD. 295 (1988) (arguing that accountant liability for negligently prepared audits is unjustified).

2. *Third-Party vs. Primary Liability*

Focusing on primary wrongdoing, the economic literature assumes that liability should make users internalize the social cost of their wrongdoing. This assumption implies that defendants should ultimately bear the losses produced by their conduct even when they are unable to prevent these losses, because internalizing these costs will induce defendants to adopt an optimal scale of activity.[35]

Third-party liability, however, is different. It is commonly accepted that the scale of third parties' activity should not be adjusted to the social cost of wrongdoing.[36] Applied to ISPs, this assumption implies that the goal of ISP liability is not to make ISPs scale down the amount of services they offer to subscribers. Rather, the goal of expanding liability to ISPs is to prevent user misconduct. Thus, in the remainder of this Article, I assume that ISPs should not internalize the social loss produced by subscriber conduct that they are unable to prevent. As my analysis of the *Napster* decisions will show, this assumption is critical for reconciling the conflicting approaches over the scope of vicarious copyright infringement.[37]

One final clarification should be made before turning to the ISP overdeterrence phenomenon. In this Article, I assume that the distinction between primary wrongdoers and third parties is clear. Internet users are assumed to be primary wrongdoers while the providers of Internet services are assumed to be third parties exposed to liability due to the failure of primary liability to prevent user misconduct.[38] In reality, however, demarcating the boundary between primary and secondary liability might prove to be a daunting analytical task.[39] I will thus return to the distinction between primary and secondary liability in Part IV.[40]

---

35 *See* discussion *infra* Part I.B.

36 *See generally* Alan O. Sykes, *The Boundaries of Vicarious Liability: An Economic Analysis of the Scope of Employment Rule and Related Legal Doctrines*, 101 HARV. L. REV. 563 (1988) (developing the notion of enterprise causation to distinguish primary and secondary wrongdoing).

37 *See* discussion *infra* Part IV.A.1.

38 *See* Yen, *supra* note 14, at 1856–65 (arguing that ISPs should be treated as third parties and thus should not internalize the cost of cyber-misconduct). *But cf.* Hardy, *supra* note 15, at 1044 (supporting strict ISP liability under the assumption that Internet service providers should adjust the scope of their services to the social costs associated with subscriber misconduct).

39 *Cf.* Robert A. Prentice, *Locating That "Indistinct" and "Virtually Nonexistent" Line Between Primary and Secondary Liability Under Section 10(b)*, 75 N.C. L. REV. 691, 712–75 (1997) (analyzing the murky distinction between primary and third-party liability for securities fraud).

40 *See* discussion *infra* Part IV.A.2 (exploring the implications of this problematic distinction for delineating the scope of vicarious liability for copyright infringement).

B. Strict Liability and ISPs: A Primer

What is the position of economic theory regarding the optimal standard of ISP liability? The starting point of the economic theory of deterrence is that wrongdoers have no incentive to forgo misconduct because they do not internalize the social harm produced by their behavior. Accordingly, the legal system should aspire to make wrongdoers pay for the harm that they cause, and thereby induce them to prevent the harmful consequences of their undesirable conduct. To achieve *optimal* deterrence, the legal system should make the expected penalty, or the amount of damages, equal to the social harm.[41] The intuition underlying this conclusion is straightforward: as the penalties make wrongdoers internalize the full social harm associated with their conduct, they will be induced to take the socially desirable steps to prevent that harm.[42] A wrongdoer would have no incentive to exercise too much care because the marginal increase in the cost of care would exceed the marginal saving in liability cost. Likewise, a wrongdoer would have no incentive to exercise too little care because the marginal increase in liability cost would exceed the marginal saving on care.

Conventional economic wisdom also prefers strict liability to negligence. Both strict liability and negligence induce wrongdoers to exercise an optimal level of care, but only strict liability would induce defendants to adjust the scope of their activity to the optimal level.[43]

---

41 *See* A. Mitchell Polinsky & Steven Shavell, *Punitive Damages: An Economic Analysis*, 111 HARV. L. REV. 869, 873–75 (1998) [hereinafter Polinsky & Shavell, *Punitive Damages*] (using this insight to justify punitive damages in limited contexts). When the probability of detection is lower than one, the optimal penalty should be such that the expected penalty remains equal to social harm. That is, the sanction should equal social harm multiplied by the inverse of the probability of detection. *See generally* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968) (making this argument in the context of public enforcement). Another justification for making penalties differ from social harm is risk aversion. When defendants are risk averse, the optimal penalty might turn out to be smaller than social harm. *See* A. Mitchell Polinsky & Steven Shavell, *The Optimal Tradeoff Between the Probability and Magnitude of Fines*, 69 AM. ECON. REV. 880, 880, 885 (1979) [hereinafter Polinsky & Shavell, *The Optimal Tradeoff*]. This Article proceeds under the assumption that ISP defendants are risk neutral. This assumption is justified for two reasons. First, to the extent that ISPs face civil liability, they might be able to purchase liability insurance. Second, some ISPs, such as AOL, are public corporations, which are assumed to be risk neutral.

42 *See* Polinsky & Shavell, *Punitive Damages*, *supra* note 41, at 879 (explaining that "[i]f damages equal harm, potential injurers will in theory have socially correct incentives to take precautions").

43 This is because strict liability makes wrongdoers pay for the full social harm produced by their conduct regardless of their level of care. *See* Jennifer Arlen & Reinier Kraakman, *Controlling Corporate Misconduct: An Analysis of Corporate Liability Regimes*, 72 N.Y.U. L. REV. 687, 692–93 (1997) (emphasizing the goal of achieving optimal level of production in setting optimal liability standards for corporations); Shavell, *supra* note 11, at 3. The endorsement of strict liability by the economic literature is manifested also in the context of corporate criminal liability. *See* Daniel R. Fischel & Alan O. Sykes, *Corporate Crime*, 25 J.

Finally, and more important for our purposes, strict liability imposes a relatively light informational burden on courts. Under strict liability, courts need only inquire about the social harm.[44] Based on their expected liability, defendants then determine what level of care to adopt.[45] Under negligence, in contrast, courts have to inquire not only about social harm, but also about the cost of care and the actual level of care exercised by the defendant.[46] Because wrongdoers are generally better positioned than lawmakers or courts to determine the appropriate level of care, strict liability is superior.[47]

The implications for ISP liability are straightforward. Under this depiction of the economic position, ISPs should face strict liability for the full social harm associated with user misconduct. Consider the liability of an Internet access provider, such as AOL, for copyright infringement by its users. Facing strict liability, the argument goes, AOL would not only exercise the socially desirable amount of effort to prevent user misconduct, but also charge optimal prices for its Internet services. Moreover, under a regime of strict liability, all that courts have to do is verify the harm caused by user misconduct. Courts should inquire into neither the actual policies adopted by AOL to prevent user misconduct nor the desirable policy of ISP monitoring.[48] This outcome is desirable because AOL is arguably better positioned than courts to determine what monitoring technology would most effectively prevent user misconduct.

Invoking the prohibitive cost of monitoring user conduct over the Internet, commentators have commonly discarded strict liability as

---

LEGAL STUD. 319, 328 (1996) (rejecting any type of "negligence-based" penalties for corporate crimes because such a regime "might allow the corporation to externalize certain social costs of doing business"); V.S. Khanna, *Is the Notion of Corporate Fault a Faulty Notion?: The Case of Corporate Mens Rea*, 79 B.U. L. REV. 355, 359 (1999) (concluding that "even though mens rea standards for individuals may prove desirable for many reasons, corporate mens rea standards are generally undesirable").

44 Steven Shavell, *Liability and the Incentive to Obtain Information About Risk*, 21 J. LEGAL STUD. 259, 269 (1992).

45 *See* Shavell, *supra* note 11, at 8.

46 *See id.* at 8–9.

47 This is because wrongdoers possess private information about their cost of care while courts would have to exercise costly effort to acquire this information. *See* Louis Kaplow & Steven Shavell, *Property Rules Versus Liability Rules: An Economic Analysis*, 109 HARV. L. REV. 713, 726–27 (1996). This insight motivates Louis Kaplow and Steven Shavell to prefer liability rules over property rules. *See id.* at 725–27 (emphasizing that, regardless of how imperfect the state's information is about harm or prevention costs, a liability rule with damages equal to average harm is superior to a property rule); *see also* Richard A. Epstein, *A Theory of Strict Liability*, 2 J. LEGAL STUD. 151, 188 (1973) (under strict liability, "[t]here is no need to ask the hard question of which branch of government is best able to make cost-benefit determinations, because the matter is left in private hands").

48 For such straightforward application of the economic theory of deterrence to ISPs, see Hardy, *supra* note 15, at 1044–46 (endorsing the imposition of strict liability on ISPs on economic grounds). This simple application of economic analysis perhaps can account for the lack of a body of economically oriented scholarship addressing ISP liability.

unsuitable for the ISP industry.[49] The argument against strict liability is basically the following: While some users indeed abuse their Internet access for committing misconduct, the majority of users rely on their Internet access to engage in legitimate activities. ISPs are unable to distinguish between legitimate and illegitimate user conduct without monitoring the information disseminated through their networks.[50] The voluminous amount of data transmitted through the Internet makes such monitoring very costly.[51] Strict liability, therefore, is undesirable because it fails to take into account the high cost of monitoring.[52]

This argument is perhaps correct in describing the high cost of monitoring user conduct. Nonetheless, it is inconsistent with economic theory. As Steven Shavell has shown, strict liability provides uninformed defendants with optimal incentives to acquire information.[53] Hence, the allegedly prohibitive cost of monitoring should not, by itself, preclude the adoption of strict liability: if monitoring is indeed too costly, ISPs will prefer to pay damages rather than bear the cost of monitoring; if monitoring is desirable, ISPs will find monitoring to be cheaper than liability costs.[54]

This Article, however, introduces a more convincing reason for questioning the wisdom of subjecting ISPs to strict liability. The dominance of strict liability has originated within the paradigm of primary liability. ISP liability, by contrast, is secondary in nature, because the primary wrongdoers are users, and not the companies providing them with Internet services.[55] In the next subpart, I shall explain why the

---

49 *See, e.g.*, Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators*, 13 CARDOZO ARTS & ENT. L.J. 345, 399–410 (1995); Yen, *supra* note 14, at 1843–72.

50 *See* Elkin-Koren, *supra* note 49, at 405.

51 *See* Yen, *supra* note 14, at 1852–53; Christian C.M. Beams, Note, *The Copyright Dilemma Involving Online Service Providers: Problem Solved . . . for Now*, 51 FED. COMM. L.J. 823, 830 (1999) (arguing that the immense size of the Web makes ISP monitoring almost impossible); R. Carter Kirkwood, Comment, *When Should Computer Owners Be Liable for Copyright Infringement by Users?*, 64 U. CHI. L. REV. 709, 711–12 (1997) (arguing that monitoring by ISPs would be "extremely expensive").

52 *See* M. David Dobbins, Note, *Computer Bulletin Board Operator Liability for Users' Infringing Acts*, 94 MICH. L. REV. 217, 227 (1995) ("Although it might be possible for a bulletin board operator to prevent infringement by . . . monitoring every upload and download to the bulletin board, requiring such control would be unrealistic and burdensome.").

53 Shavell, *supra* note 44, at 260; *see also* Louis Kaplow, *Optimal Deterrence, Uninformed Individuals, and Acquiring Information About Whether Acts Are Subject to Sanctions*, 6 J.L. ECON. & ORG. 93 (1990) (applying similar analysis to study the effort to obtain information about law).

54 To be sure, the degree to which ISPs can successfully monitor user conduct is relevant for the decision to expand liability to ISPs. If they are unable to detect user misconduct, subjecting ISPs to liability might be unjustified. *See supra* text accompanying note 33.

55 For a discussion of this assumption, see *supra* text accompanying notes 35–37.

status of ISPs as third parties is significant in producing overdeterrence under strict liability.

C. On Divergent Incentives and Overly Zealous ISPs

The existing economic understanding outlined in the preceding subparts raises the first doubt over imposing strict liability on ISPs. As ISPs are not considered to be the primary wrongdoers, they should not internalize the social cost of user misconduct. Hence, the optimal-production objective of strict liability should not be extended to ISP liability.[56] Current understanding, however, leaves intact the insight that strict liability will induce service providers to engage in the desirable level of effort to police subscriber misconduct. This subpart challenges this insight and argues that, given the different incentive structure facing primary wrongdoers and third parties, imposing strict liability on ISPs would result in overdeterrence in the form of excessive monitoring by ISPs and overzealous censorship policies. In this subpart, I identify and analyze the third-party overdeterrence problem. In the next Part, I will review in depth the causes and the limits of this overdeterrence phenomenon.

1. *The Divergent Incentives of Third Parties*

This section argues that subjecting ISPs to strict liability induces them to monitor excessively against subscriber misconduct and overzealously censor materials suspected of being illegitimate. The analysis applies to many scenarios in which: (1) from a pure technical perspective, the third party exercises control over the conduct of the primary wrongdoer and is thus positioned to prevent misconduct independently, without the cooperation of the primary wrongdoer; and (2) the cost borne by the third party for preventing the conduct is negligible. For expositional convenience, however, the remainder of this section will analyze the liability of web-hosting service providers for their subscribers' copyright infringement.

Maintaining a website requires website owners to store the website information on a server, which would be accessible to visitors through the Internet. Web-hosting companies provide physical space on their servers where users can store their website data. The subscriber designs the site, determines what materials to post and what activities will be offered to visitors, whereas the web-hosting ISP is usually paid according to the storage space assigned to the subscriber and

---

56 Imposing strict liability may lead to overdeterrence to the extent that third parties will unjustifiably scale down their level of production. *See* Sykes, *supra* note 36, at 578–79 (arguing that negligence standards should be imposed on third parties because the goal of optimal production is inapplicable).

the volume of traffic the site generates.[57] Assume that the subscriber posts photographs on his website, some of which might be unauthorized copies of copyrighted material. Because it stores the website data, the ISP is technically capable of preventing all copyright infringement by removing infringing items from its servers. Moreover, the cost of removing a given photograph by the ISP is virtually zero. To prevent only infringing conduct, however, the ISP must examine the photographs posted by the user and determine which ones are infringing and which ones are not. The thesis that I offer is that, under strict liability for copyright infringement, the ISP will adopt an overly aggressive monitoring policy, and remove too many legal photographs from its users' sites.

Unlike the primary wrongdoers depicted by the economic literature, ISPs do not capture the full value of the conduct they are entrusted with policing. While economic theory assumes that wrongdoers do not internalize the losses associated with their conduct, it does assume that wrongdoers capture the benefits of their conduct.[58] Under this view, strict liability, which makes wrongdoers internalize the full social cost of their conduct, aligns private incentives with social interest. Once wrongdoers internalize both full social cost and social gain produced by their conduct, they will be induced to take the socially optimal steps to prevent harm. However, this key assumption does not necessarily hold with respect to third parties, who do not always capture the full value of the conduct they are obliged to monitor.[59] In our example, web-hosting service providers do not capture the full value of each photograph posted by their subscribers on their servers. Rather, the ISP is paid a fixed fee, which depends on the space used by the subscriber. Given this "positive ex-

---

57 Earthlink, for example, charges a fixed fee that varies according to the storage space provided and the amount of traffic allowed. For example, as of January 19, 2002, the monthly fee for 175 megabytes of storage space and traffic limit of 10 gigabytes has been $19.95. *See* Earthlink, Inc., Web Hosting Packages, *at* www.earthlink.com/business/ecommerce/smartsite.html (last visited Jan. 19, 2002). Some ISPs, AOL for example, provide their users with limited free web-hosting services. AOL Time Warner Inc., AOL Home Page, *at* http://www.aol.com (last visited Jan. 19, 2002). The conclusions of this Part apply, perhaps with even greater force, to these types of hosting services.

58 *See generally* Keith N. Hylton, *A Missing Markets Theory of Tort Law*, 90 NW. U. L. REV. 977 (1996) (noting that assumption and exploring its implications). My argument differs from Hylton's in several respects. First, Hylton limits his discussion to primary wrongdoing and therefore attributes the lack of internalization to the existence of thin markets. This Article, in contrast, explores the link between third-party liability and the lack of internalization of benefits. Second, Hylton advocates the adoption of negligence rules and overlooks other plausible strategies identified in this Article.

59 This Article does not address another type of cost potentially ignored by service providers—the loss of network benefits produced by blocking access to the Internet. *See* Katyal, *supra* note 4, at 1084–87, 1098–99 (arguing that victims and ISPs will not take into account the network benefits associated with Internet use and, thus, might engage in overprecaution).

ternalities" problem, the conventional prescription of economic analysis—set penalties to equal social harm—would result in overdeterrence, the adoption of overly aggressive monitoring policies, and excessive censorship practices by ISPs.

2. *In-House Hosting*

To illustrate the ISP overdeterrence phenomenon, it would be useful to contrast a scenario in which subscribers use their own computers to host their website with a scenario in which subscribers contract with ISPs for hosting services. This section shows that the monitoring and censorship practices employed by a subscriber who uses in-house hosting would be optimal under a regime of strict liability for copyright infringement. The next section shows that imposing identical liability on an ISP would produce excessive censorship.

Assume that a website owner uses her own computer systems to host her website. The owner faces strict liability for any unauthorized photograph posted on that site, and must decide what level of monitoring to exercise to verify the legal status of such photographs.[60] As the standard economic account shows, the website owner would adopt the socially optimal level of monitoring.[61] To be sure, under conditions of costly information, the optimal level of monitoring might result in the removal of perfectly legal photographs from the server.[62] Yet, as long as the owner internalizes both the social value of the content that she posts on her site and the social harm associated with copyright infringement, the amount of legal photographs removed would be optimal.

The following example demonstrates this argument. The value of each photograph posted on the site is 200. The penalty for posting a copyrighted photograph without permission equals social harm,

---

60 I assume that the owner would not post copyrighted photographs that she knows to be infringing without permission because the penalty for copyright infringement exceeds the benefits from posting such photographs. *See infra* text following note 111 (elaborating on that assumption and analyzing its implications for choosing alternatives to strict liability).

61 *See* Shavell, *supra* note 44, at 260 (asserting that strict liability induces defendants to adopt optimal level of investment in acquiring information).

62 This will be the case when the cost of obtaining additional information exceeds the expected value of this information. Consider the following example: Having acquired some information about photograph A, the owner believes the likelihood this photograph is infringing is 70%. The social harm from infringement, as well as the sanction for infringement, equals 100. The value of posting the photograph is 50. Further investigating the legal status of the photograph would cost 150. It is therefore evident that further inquiring is not desirable because the cost of such inquiry exceeds the value of posting the photograph. Given the uncertainty over the infringing nature of the photograph, however, it is desirable not to post it, because the expected harm from infringement, 70, exceeds the value of posting the photograph. This would be the case even if, in hindsight, it turned out the photograph had been perfectly legal.

1000. The probability that any given picture is infringing is 0.1. The owner needs to choose between two alternative monitoring technologies:[63] Technology A, which is known to detect only 50% of infringing photographs, costs 20 per photograph examined. Technology B, known to detect 60% of infringing photographs, also entails a cost of 20 per photograph. This technology, however, would incorrectly identify 10% of the legal copies as illegal. Table 1 summarizes the owner's costs and benefits from adopting the two technologies.

TABLE 1: MONITORING DECISION BY A SINGLE ENTITY

Technology	Expected Cost	Expected Benefit	Net Value
None	100	200	100
A	20+50=70	200–10=190	120
B	20+40=60	200–18–12=168	110

The owner's expected value from posting a photograph on the site equals the expected benefit of the photograph minus the expected liability for copyright infringement. Without adopting any of the technologies, the owner's expected value of operating the site is 100 ($200 - 0.1 \times 1000$). Adopting Technology A leaves the owner with an expected value of 120 ($200 - 20 - 0.5 \times 0.1 \times 200 - 0.5 \times 0.1 \times 1000$). Adopting Technology B leaves the owner with an expected value of 110 ($200 - 20 - 0.6 \times 0.1 \times 200 - 0.1 \times 0.9 \times 200 - 0.4 \times 0.1 \times 1000$). The owner will undoubtedly choose the first monitoring technology. As economic theory projects, Technology A is also the socially optimal one.

3. *Outsourced Hosting*

The technology adopted to identify infringement will differ if the website owner contracts with an ISP for hosting services.[64] For simplicity, assume that the owner is judgment-proof and therefore exer-

63 Making the website owner choose between two monitoring technologies rather than reach individual decisions for each picture is consistent with practice, where the emerging trend is automating the process of monitoring and screening rather than exercising individual judgment. The process of automated monitoring for unlawful content is commonly known as filtering. *See* R. Polk Wagner, *Filters and the First Amendment*, 83 MINN. L. REV. 755, 757 (1999). While this trend may not reflect the actual practices of individual website owners, it definitely reflects the practice of ISPs, who must monitor large volumes of information and traffic. Of course, the text's focus on monitoring technology does not undermine the generality of the argument that incentive divergence leads to overdeterrence.

64 The decision to contract for services rather than perform them within the boundaries of the firm has been extensively studied by the economic literature. *See, e.g.*, OLIVER HART, FIRMS, CONTRACTS AND FINANCIAL STRUCTURE 21–28 (1995) (reviewing economic approaches to the issue); R.H. Coase, *The Nature of the Firm*, 4 ECONOMICA 386, 398–405 (1937). In this Article, I take this decision to be exogenous, i.e., unaffected by considera-

cises no effort to investigate the legal status of the materials posted on her site, and that the ISP is paid a fixed fee according to the storage space assigned to the user. To prevent online copyright infringement, the legal system imposes liability on ISPs whenever the materials stored on their servers, the photographs posted by the subscriber in our example, are infringing. Table 2 summarizes the costs and benefits of the two technologies from the perspective of the ISP.

TABLE 2: MONITORING BY AN ISP

Technology	Monitoring Cost	Liability Cost	Total Costs
None	0	100	100
A	20	50	70
B	20	40	60

As the ISP is paid a fixed fee, it captures no value from allowing an additional photograph to be stored on its servers. The ISP therefore does not take into account the cost of monitoring produced by the removal of photographs from the website it hosts. On the other hand, the ISP faces strict liability for the full social harm caused by user infringement. As a result, the ISP would adopt the second, non-optimal monitoring technology.[65] Under no monitoring, the expected cost for the ISP equals its expected liability. The value of monitoring for the ISP consists of its reduction in expected liability costs. Thus, adopting Technology A leaves the ISP with an expected cost of 20 + 50 = 70. Adopting Technology B leaves the ISP with an expected cost of 20 + 40 = 60. Thus, the ISP would adopt the second, overly aggressive technology.

The choice of Technology B by the ISP is the outcome of the different incentives faced by the subscriber, the primary wrongdoer, and the ISP, the third party. Were it to choose a monitoring technology, the primary wrongdoer would take into account not only expected social harm and the actual cost of monitoring, but also the cost associated with the removal of non-infringing photographs from the website. The ISP decision, by contrast, is not affected by the value of items removed due to the inaccuracy of the monitoring technology.

---

tions of expected liability. *But see* discussion *infra* text following note 91 (relaxing somewhat this assumption).

65 The overdeterrence problem caused by strict liability mirrors the alleged overdeterrence caused by subjecting corporate managers to personal liability. *Cf.* Bruce Chapman, *Corporate Tort Liability and the Problem of Overcompliance*, 69 S. CAL. L. REV. 1679, 1687–94 (1996) (arguing that because the cost of managerial care is borne by shareholders, imposing strict liability on managers will induce them into overcompliance); Jonathan R. Macey, *Agency Theory and the Criminal Liability of Organizations*, 71 B.U. L. REV. 315, 319 (1991) (emphasizing that managerial liability could lead to overdeterrence of managers because of managerial risk aversion).

The overdeterrence of ISPs can take two forms. First, as illustrated in the numerical example, the ISP would tend to apply an overly aggressive monitoring technology that would excessively remove materials from the Internet. Second, the ISP might decide to pay an excessive price for purchasing and implementing a monitoring technology (our example assumed that monitoring technologies equal in their actual costs and differ only with respect to their level of accuracy).

The key implication of the ISP overdeterrence phenomenon is that, contrary to conventional wisdom, the legal system cannot limit its role to imposing penalties that equal social harm, yet still rely on the information held by defendants to make them take optimal care. Since third parties do not internalize the full social value of the underlying activities, making them pay for full social harm would result in overcompliance. In Part III, I elaborate on the legal mechanisms that could eliminate the risk of excessive censorship while promoting the goal of preventing user misconduct. First, however, I shall explore in depth the sources for the divergent incentives of ISPs and their subscribers.

II
THE INCENTIVE-DIVERGENCE THESIS

The conclusion of the preceding Part can be stated as follows: When the incentives of the third party diverge from those of the primary wrongdoer, imposing liability on the third party might result in overdeterrence. This observation generates two conflicting responses. The first approach, which I shall label the "restrictive approach," invokes the divergence of incentives to support broad restrictions on third-party liability. Members of the restrictive camp question the constitutionality of third-party liability and argue, for example, that third-party liability should be imposed only where the courts have predetermined that the conduct is unlawful.[66] The second approach, which I shall label the "market approach," argues that the risk of overdeterrence is overstated because market forces, especially competition in the market for Internet services, would align the incentives of primary wrongdoers and third parties.[67] The logic underlying the

66 *See, e.g.*, Michael I. Meyerson, *Authors, Editors, and Uncommon Carriers: Identifying the "Speaker" Within the New Media*, 71 NOTRE DAME L. REV. 79, 122 (1995) (arguing that third parties should "only be responsible for distributing the speech of another if they have 'actual notice' that the speech has previously been adjudicated illegal or unprotected"); *see also supra* note 16 (making similar points with respect to employer liability for sexual harassment in the workplace).

67 Though this approach has not been explicitly stated in the ISP context, it mirrors the approach of the Chicago School to the agency problem in corporate law. Under this approach, competition in the markets for capital, products, and managerial services will drive the management of public corporations to take shareholder interest into account.

market approach is simple. ISPs compete to attract subscribers. Subscribers would prefer to purchase services from ISPs that do not engage in excessive censorship. As a result, ISPs wishing to attract users would not adopt overly zealous censorship practices. Thus, the market, and not modifying liability rules, will be most effective in eliminating overdeterrence.

I find both categorical approaches to be flawed. Both approaches adopt a uniform view of the third-party overdeterrence phenomenon, under which all instances of third-party liability should receive identical treatment. In contrast, this Article posits that the magnitude of the overdeterrence problem varies across services offered by third parties. In this Part, I seek to enhance the understanding of the overdeterrence phenomenon by developing a framework that would enable policymakers to distinguish various types of third parties and tailor legal solutions accordingly. First, I analyze the causes for the divergence of incentives between third parties and primary wrongdoers, and show why a categorical market approach might be flawed. Second, I highlight conditions that might mitigate the overdeterrence phenomenon, and therefore suggest that the restrictive approach is also unsatisfactory.

A. Transaction Costs and the Market Approach

This subpart explores the causes for the divergence of incentives between ISPs and their subscribers. As will be shown, the basic intuition underlying the market approach is correct. The mutual interest of the parties ex ante is indeed to commit the ISP to optimal screening and censorship practices. What the market approach misses, however, is that transaction costs of different types might prevent the parties from achieving privately this desirable outcome and eliminating the risk of overzealous censorship by ISPs. Moreover, some of these impediments to the ability of the parties to resolve the problem are the product of legal rules. Rather than leaving market forces to eliminate the risk of overdeterrence, an optimal regime of ISP liability must devise strategies to overcome these impediments.

To uncover the roots of the ISP overdeterrence phenomenon, it might be useful to think about the relationship between users and ISPs in terms of a principal-agent relationship. The principal, the subscriber, hires the agent, the ISP, to host its webpage for a fee. The agent can act independently to prevent the principal's misconduct.[68]

For prominent advocates of this approach, see Frank H. Easterbrook & Daniel R. Fischel, *The Corporate Contract*, 89 COLUM. L. REV. 1416, 1447 (1989); and Ralph K. Winter, Jr., *State Law, Shareholder Protection, and the Theory of the Corporation*, 6 J. LEGAL STUD. 251, 289 (1977).

68 In fact, imposing liability on the ISP produces two parallel sets of principal-agent problems. First, the subscriber might engage in illegal activity, and thereby subject the ISP

Because the agent faces liability for the actions of the principal, it would be too cautious whenever its incentives are not aligned with those of the principal. This subpart explores the extent to which the interests of the parties can be aligned.

The starting point is that, like in many other principal-agent relationships, the mutual interest of the parties ex ante is to commit the ISP to optimal monitoring policy, because such commitment would maximize the joint surplus produced by the transaction.[69] The previous web-hosting example illustrates this mutual interest of the parties. When the ISP adopts the optimal monitoring technology, A, the expected benefit to the subscriber is 190 (the value per photograph of 200, multiplied by the expected number of photographs, or 0.95), while the expected cost for the ISP is 70 (monitoring cost of 20, plus expected liability cost of 50). When the ISP adopts the suboptimal monitoring technology, B, expected subscriber benefit is 170 (200 × 0.85), whereas the expected cost for the ISP is 60 (20 + 40). Switching from Technology B to Technology A adds to the subscriber an expected benefit of 20 (190 – 170), while increasing the expected liability of the ISP only by 10. In a world of zero transaction costs, the subscriber would be willing to indemnify the ISP for its increase in expected liability, 10, and, depending on the bargaining power of the parties, offer the ISP up to 10 in return for a commitment to the optimal level of monitoring. Table 3 summarizes the net value of the two monitoring technologies.

TABLE 3: NET VALUE OF MONITORING TECHNOLOGIES

Monitoring Technology	ISP Cost	User Benefit	Net Surplus
A	20+50=70	200(1–0.05)=190	190–70=120
B	20+40=60	200(1–0.06–0.09)=170	170–60=110

Despite their mutual interest, the parties may fail to contract effectively on the optimal ISP monitoring policy because of the existence of transaction costs. The market approach should be

to legal liability. This is the standard description of the relationship between third parties and primary wrongdoers. *See generally* Steven Shavell, *On Liability and Insurance*, 13 BELL J. ECON. 120 (1982) (describing the relationship between liability insurers and wrongdoers along the principal-agent paradigm). This Article highlights the second principal-agent problem: that the ISP might be too cautious and excessively censor the information that the subscriber stored on its server.

69 More generally, in the absence of transaction costs the allocation of liability between third parties and primary wrongdoers does not matter. The parties will privately shift liability to the optimal target. For the application of this insight in the context of vicarious liability in tort, see Lewis A. Kornhauser, *An Economic Analysis of the Choice Between Enterprise and Personal Liability for Accidents*, 70 CAL. L. REV. 1345, 1347–49 (1982); and Sykes, *supra* note 27, at 1233–79.

abandoned if altering the rules of ISP liability is cheaper than the cost faced by the parties in overcoming these transaction costs.[70] In addition to the standard costs of negotiating the agreement and putting it into writing, three unique types of transaction costs characterize the ISP-subscriber relationship, and prevent the parties from contracting effectively on the level of monitoring exercised by the ISP: ex post negotiation costs, informational problems, and legal impediments.

1. *Ex Post Negotiation Costs*

Ex post negotiation costs measure the ability of the parties to negotiate the filtering of specific items rather than general monitoring policies. In the web-hosting example, the subject of ex post negotiations will be the removal of a specific photograph from the subscriber's website, rather than the overall censorship policy guiding the ISP. If the parties can negotiate on the terms of each removal, the subscriber might be able to offer the ISP a payment to induce it to take into account the benefits of each relevant item. The ability to negotiate cheaply over specific items also enables the parties to exchange information about the legal status of specific items and to convince the ISP that no legal risk is involved.

The ability to negotiate ex post varies across Internet services. In the web-hosting case, the parties might find it relatively easy to negotiate about the removal of specific items. This is because the subscriber will immediately learn about the removal of such items,[71] and the ISP will have only one party with whom to negotiate. By contrast, the cost of ex post negotiations between Internet access providers and their subscribers might be prohibitive. Consider the case in which an Internet access provider blocks access to a particular site it suspects to be engaging in copyright infringement. This decision affects all users who rely on that ISP to provide them with Internet access. The *collective* interest of these users, as a group, in having access to this site might outweigh the ISP's risk of legal liability. Nevertheless, an individual user will decline to take the time and the effort to negotiate with the ISP and convince it to enable access to the site as long as its *personal* stake in access to that site is smaller than the cost of such

---

70 *Cf.* Kraakman, *supra* note 31, at 866–67 (making this argument in the context of managerial liability); *see also* A. Mitchell Polinsky & Steven Shavell, *Should Employees Be Subject to Fines and Imprisonment Given the Existence of Corporate Liability?*, 13 INT'L REV. L. & ECON. 239 (1993) (justifying criminal liability of corporate employees when their limited wealth makes the state, through the use of imprisonment sanctions for unpaid criminal fines, more effective than employers in providing employees with incentives to avoid misconduct).

71 *See infra* text accompanying notes 74–76 (discussing informational problems in observing removal decisions).

negotiations. This collective action problem thus substantially increases the cost of negotiating ex post with access providers.[72]

2. *Informational Problems*

Assume that a web-hosting contract specifies the monitoring policy to be adopted by the ISP. Such a contract would identify, for example, the monitoring technology to be adopted by the ISP, and the conditions under which an item can be removed from the ISP's server. Once the contract is in effect, however, the ISP has a clear incentive to renege on its contractual promises and adopt an overly aggressive monitoring policy in order to minimize its exposure to legal liability.[73] To enforce the ISP's contractual obligations, the subscriber must be able to overcome two informational hurdles: (1) observe the actual monitoring policy employed by the ISP; and (2) prove in court that the actual monitoring policy differs from the one agreed upon in the contract.[74]

Observing the actual monitoring policy adopted by the ISP can be very costly for subscribers. Consider again the web-hosting example. The subscriber will most likely learn about the removal of specific photographs from her site, but she cannot simply deduce the general monitoring policy guiding the ISP by merely observing individual removal decisions. Rather, she will have to invest costly time and effort to uncover the monitoring policy underlying the ISP's specific removal decision. This task would be particularly tricky when monitoring is performed through a combination of technology and human judgment.[75] Furthermore, whereas subscribers for web-hosting ser-

---

72 The costs associated with collective bargaining problems have been relied upon, in the context of eminent domain, to justify a liability rule that substitutes court-assessed damages for private bargaining. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1106–10 (1972). In our context, this prescription implies that lawmakers should adopt a rule under which ISPs would compensate users for the wrongful removal of items. As described *infra* Part IV.B, however, the law fails to provide such a rule, and in fact grants immunity to ISPs that remove subscribers' materials.

73 The text relies on the assumption made earlier that the fixed fee is paid at the early stage of the contract. The analysis also abstracts from mechanisms that might be adopted by the parties to provide the ISP with self-enforcing incentives to induce it to deliver on its promise to maintain a relaxed monitoring policy. On the implications of self-enforcing incentives, such as fee-sharing agreements, for the design of liability, see *infra* Part III.

74 Economic analysis of principal-agent relationship focuses mostly on the ability of the principal to observe the agent's conduct. *See, e.g.*, ANDREU MAS-COLELL ET AL., MICROECONOMIC THEORY 482 (1995) (arguing that the ability of the principal to observe agent effort leads to first-best outcome). However, in the absence of self-enforcing mechanisms, contractual disputes might require not only observability by the principal, but also legal enforcement, thus requiring the principal to prove its case in court.

75 EBay, for example, employs a combination of automated monitoring and manual operations to prevent sales that infringe copyright. *See* Glenn R. Simpson, *EBay to Police Site for Sales of Pirated Items*, WALL ST. J., Feb. 28, 2001, at A3.

vices and people posting items for sale on auction sites might learn quickly about the removal of their materials from the Internet, subscribers of other services might find it challenging not only to observe general monitoring policies, but also to learn about specific items screened out by their ISP. A user may be unaware of her Internet access provider's decision to block access to a specific web address. Similarly, employers can block incoming E-mails they deem to be inappropriate without notifying their employees. Outgoing messages from Microsoft's Hotmail E-mail service, for example, had failed to reach their destination for several months before subscribers learned these failures were intentional, part of a filtering policy adopted by Microsoft.[76] Needless to say, the hurdle of proving the ISP's actual monitoring policy in court is obviously more difficult to overcome than the hurdle of privately observing the actual monitoring policy.

3. *Legal Obstacles*

The legal system might impose two additional obstacles on private contracting for relaxed monitoring policies. First, contractual commitment to limit monitoring and censorship effort undermines the ISP's position in future litigation over its failure to remove infringing material. It would be an uphill battle for an ISP to argue convincingly that it did all that it could to prevent misconduct by users when, in its contract with users, it promised not to engage in fierce monitoring.[77]

Second, the legal system might impose difficulties on users trying to sue ISPs for damages associated with removing their materials from the Internet. Both the Digital Millennium Copyright Act[78] and the Communications Decency Act,[79] for example, grant ISPs effective immunity from liability for the removal of materials suspected of being

---

76 In its effort to fight spam, Microsoft has blocked outgoing mails from its Hotmail service to websites hosted by ISPs who were commonly associated with spam. Lisa M. Bowman, *Hotmail Spam Filters Block Outgoing E-Mail*, CNET NEWS.COM, Jan. 18, 2001, *at* http://news.cnet.com/news/0-1005-201-4523924-0.html. Microsoft did not inform its users about its policy. *Id.* This policy was discovered only several months after it had been adopted. *See id.*

77 In the *Netcom* case, for example, plaintiffs posited that Netcom, a provider of web-hosting services, developed a reputation for its refusal to monitor against copyright infringement and advertised promising "a regulation-free" service. *See* Religious Tech. Ctr. v. Netcom On-Line Comm. Servs., 907 F. Supp. 1361, 1377 (N.D. Cal. 1995). Plaintiffs asked the court to rely on these arguments to find that Netcom has a financial interest in the infringing activity of its subscribers and thus hold it vicariously liable for copyright infringement. *See id.* The court, however, held that such facts do not establish the requisite "financial interest." *Id.*

78 17 U.S.C. § 512(g) (Supp. V 1999).

79 47 U.S.C. § 230(c) (Supp. V 1999).

unlawful.[80] This immunity further decreases the likelihood that subscribers would succeed in making ISPs adopt optimal censorship and filtering policies.

B. Market Incentives and the Restrictive Approach

The market approach is misguided because it overlooks the contractual impediments that prevent the parties from successfully tackling the overdeterrence problem. The restrictive approach, by contrast, overlooks the role of market incentives in mitigating the overdeterrence phenomenon. Two mechanisms may operate to align the incentives of the ISPs and subscribers: (1) contractual incentives; and (2) competition in the market for Internet services.

1. *Contractual Incentives*

The parties might be able to structure a spectrum of contractual incentives to induce ISPs to behave in an optimal manner. The economic theory of contracts explores in depth various contractual solutions to the divergence of incentives between principals and agents.[81] The benchmark mechanism for inducing the ISP to exercise optimal monitoring is providing it with the right to the residual revenues generated by the website, and leaving the subscriber with a fixed income.[82] This mechanism is self-enforcing, and eliminates the need for acquiring information about the ISP's actual monitoring policy.

It is highly unlikely that the risk of liability will be powerful enough to induce ISPs and subscribers to adopt this radical solution.[83] Nevertheless, some Internet services might exhibit, due to various business considerations, profit-sharing arrangements between subscribers

---

80 For a review of the relevant sections and their implications, see *infra* notes 171–78 and accompanying text.

81 For a general overview, see MAS-COLELL ET AL., *supra* note 74, at 477–88.

82 *See, e.g.*, Armen A. Alchian & Harold Demsetz, *Production, Information Costs, and Economic Organization*, 62 AM. ECON. REV. 777, 793 (1972); Bengt Holmstrom, *The Firm as a Subeconomy*, 15 J.L. ECON. & ORG. 74, 79 (1999).

83 This benchmark mechanism is unlikely to be adopted for several reasons. First, it creates a parallel moral hazard problem that might prove to be more severe than the ISP overcompliance problem. To ensure that subscribers put forth sufficient efforts to attract traffic to their websites, an ISP would be forced to monitor its subscribers' activities. Given that business considerations dictate the structure under which the website owner contracts with the service provider with a fixed fee, this reverse moral hazard problem is probably more severe than the one produced by ISP liability. Finally, this solution is inapplicable in the context of Internet access providers, and in any other scenario in which the subscriber does not contract with the ISP for commercial purposes. More generally, this Article assumes that changes in legal rules would not affect the ways in which the parties structure their transactions. *See supra* note 64 (making the assumption that a firm's decision to contract for services rather than perform them internally is unlikely to be affected by considerations of expected liability).

and ISPs. Consider the case of auction websites.[84] These sites charge fees that vary in proportion to the sale price of the items sold through the site. Profit-sharing agreements of this type constitute a self-enforcing mechanism to mitigate the divergence of incentives between the parties. Each item removed by the auctioning website produces a revenue loss in proportion to the value of the item removed. Thus, with some adjustments in the magnitude of the penalties, imposing strict liability on auction websites may result in optimal monitoring effort.[85]

2. *Competition*

Competition in the market for Internet services indeed constrains ISP overdeterrence.[86] To illustrate, consider two ISPs competing in the market for hosting services: "Censorlink, Inc." and "Zero Policing, Inc." If Censorlink goes too far in censoring materials, subscribers might switch to Zero Policing, who would employ less stringent monitoring policies and charge subscribers higher fees. However, as in the context of the shareholder-manager agency problem, competition cannot fully eliminate the divergence of incentives between ISPs and their subscribers.[87]

Two major obstacles limit the extent to which competition in the market for Internet services can align the incentives of service providers and subscribers: (1) transaction costs; and (2) the limited significance of monitoring in choosing Internet service providers. To begin, subscribers will switch from Censorlink to Zero Policing only if they expect Zero Policing to monitor less aggressively than Censorlink. But sheer contractual promises cannot credibly commit Zero Policing to a monitoring policy that would be less stringent than the one adopted by Censorlink, because the transaction costs that prevent ISPs

---

84 *See infra* Part IV.C (discussing the optimal liability of auction websites). Note, however, that existing legal rules may increase the cost of profit-sharing arrangements. By sharing in the profits of its subscribers, an ISP might be found vicariously liable for copyright infringement. *See infra* Part IV.A (discussing the doctrine of vicarious infringement).

85 This logic might also explain why the risk of excessive censorship is less significant in the analogous context of newspaper publishers, who face strict liability for the defaming stories of their reporters. Like ISPs, newspaper publishers are induced by the threat of liability to censor the speech of others, their reporters. Unlike ISPs, however, newspaper publishers, and not their reporters, derive most of the residual gains associated with the information published in the newspaper. *But see* J.M. Balkin, *Free Speech and Hostile Environments*, 99 COLUM. L. REV. 2295, 2301 (1999) (explaining the imposition of strict liability on newspaper publishers and publishing houses as an extension of vicarious liability in torts).

86 *Cf.* Mark J. Roe, *Rents and Their Corporate Consequences*, 53 STAN. L. REV. 1463 (2001) (exploring the effect of the degree of competition in the market for products on the magnitude of the incentive divergence between managers and shareholders of public corporations).

87 *Cf.* Lucian Arye Bebchuk, *Federalism and the Corporation: The Desirable Limits on State Competition in Corporate Law*, 105 HARV. L. REV. 1435, 1462–70 (1992) (reviewing the limited effect of market competition on the managerial agency problem in the context of incorporation decisions).

and subscribers from contracting on ISP monitoring policies characterize all ISPs offering similar services. To lure the subscribers of Censorlink, Zero Policing would thus have to establish a reputation for lax monitoring policies.[88] Such reputation, however, is not only difficult to establish, but also puts the ISP at a greater risk of legal liability.[89]

Even when subscribers can differentiate between ISPs based on their monitoring policies, competition might not necessarily result in the transition of subscribers to Zero Policing. ISPs compete not only on monitoring policies but also, and more importantly, on aspects such as the quality of their network, bandwidth, and prices. The best ISPs in terms of quality of services and bandwidth might be the ones employing the most cautious monitoring policies. Moreover, many Internet services, especially Internet access, are provided incidentally to another transaction or service. American universities, for example, usually provide their students and faculty with Internet access, and so do many workplaces with respect to their employees. Because the quality of Internet services is not the major factor in choosing an academic institution, universities face virtually no market incentives to converge on the optimal level of monitoring.[90]

Finally, even under the assumption that Zero Policing monitors less aggressively, a Censorlink subscriber will not switch to Zero Policing unless the switching cost is smaller than the expected value of the relaxed monitoring policy.[91]

To be sure, ISPs cannot go too far. Adopting an extremely overzealous monitoring policy increases the likelihood of subscribers' being informed about such policy, and might thus create a negative reputation for an ISP, which in turn would encourage its users to ex-

---

88 *See generally* Benjamin Klein & Keith B. Leffler, *The Role of Market Forces in Assuring Contractual Performance*, 89 J. POL. ECON. 615 (1981) (exploring the conditions for effective reputation-building).

89 *See supra* note 77. Moreover, ISPs with reputations for relaxed monitoring policies might attract many subscribers with unlawful intentions. This will increase expected liability costs for the ISP, which in turn will increase the fees they charge their users. As a result, legitimate Internet users unwilling to pay high fees will switch to ISPs that employ relatively stringent monitoring policies.

90 It seems that the major constraint on adopting overly restrictive censorship policies by academic institutions is the risk of adverse publicity. When the *Napster* case was still at its early stages, many universities blocked their students' access to Napster's site. *See* John Borland, *Metallica, Dr. Dre Urge Colleges to Cut Napster Access*, CNET NEWS.COM, Sept. 8, 2000 (reporting that, out of fifty universities surveyed, thirty-four percent blocked access to Napster), *at* http://news.cnet.com/news/0-1005-200-2728170.html. Once the interest of the media intensified, universities declined music industry requests to block such access. *See* Sam Costello, *Reading, Writing, and Napster*, INDUSTRY STANDARD, Sept. 22, 2000 (reporting the refusal of universities to block access to Napster due to concerns over censorship and academic freedom), *at* http://www.thestandard.com/article/display/0,1902,18790,00.html.

91 In the web-hosting example, the subscriber will switch ISPs only if switching costs are lower than 10.

periment with other service providers. In the web-hosting example, if overzealous monitoring is sufficiently costly, companies might opt to bear the cost of shifting to in-house web-hosting. Even in the case of incidental providers of Internet services—universities, for example—sufficiently large losses produced by excessive monitoring will make some users access the Internet through commercial ISPs.

To summarize, both categorical approaches, the market and the restrictive approach, should be rejected. Ex ante, subscribers and service providers would like to adopt the desirable level of screening. Various impediments, however, limit the ability of these parties to achieve the desirable outcome. The nature and the magnitude of the overdeterrence phenomenon vary across different types of services offered by third parties. As the next Part shows, these differences reflect on the optimal legal solution to the overdeterrence problem.

III
LEGAL STRATEGIES

Given the overdeterrence associated with strict liability, this Part explores three distinct models of legal response aimed at facilitating an optimal regime of ISP liability notwithstanding the divergence of incentives between ISPs and their subscribers. These models include: (1) scaling down penalties imposed on ISPs under strict liability; (2) regulating the ISP-subscriber interface; and (3) making the state specify the required level of ISP monitoring, either through "negligence-based" standards, or through a "monitoring-regnlation" regime. These models differ in the strategy they adopt to alleviate the risk of overdeterrence. The analysis will explore the strengths and vices of each model, and evaluate their prospects of securing the optimal level of ISP monitoring and censorship.

A. Strict Liability with Scaled-Down Penalties

At first glance, the response to the overdeterrence produced by the divergence of incentives between ISPs and their subscribers should be simple. The best response, one might argne, is to impose strict liability on ISPs but reduce the magnitude of penalties they will have to pay.[92] This response, the argument goes, would maintain the informational advantages of strict liability, but eliminate the risk of overdeterrence.[93] This argnment, though initially appealing to the economically oriented mind, is misguided. Reducing the penalties

92 *See, e.g.*, Polinsky & Shavell, *The Optimal Tradeoff*, *supra* note 41, at 886–88 (calling for decreasing the magnitude of penalties to cope with overdeterrence produced by defendants' risk aversion).

93 On the informational advantages of strict liability, see *supra* text accompanying notes 46–47.

under strict liability would achieve optimal deterrence only under very limited circumstances, namely, where profit-sharing agreements exist between ISPs and subscribers.

To examine the effect of combining strict liability with reduced penalties, let us return to our web-hosting example. In that example, the underlying assumption was that the ISP is paid a fixed fee and thus derives no marginal benefit from an increase in the number of photographs posted by the subscriber. That being the case, the ISP overdeterrence phenomenon would persist as long as the penalties imposed on the ISP are positive. This is because, at the margin, removing photographs is costless whereas liability costs are positive. Stated differently, the ISP loses nothing from removing subscriber photographs from its servers up to the point where overly aggressive censorship would induce subscribers to take their business elsewhere. On the other hand, each additional photograph suspected of being infringing increases the ISP's exposure to liability. Thus, as long as its actions do not induce its subscribers to switch service providers, the ISP would rather remove suspected photographs than face penalties, however small they might be. Scaling down the penalties for strict liability would therefore fail to ensure optimal deterrence.[94]

Strict liability with scaled-down penalties will result in optimal deterrence only when, at the margin, the ISP suffers a loss from removing each additional item from its servers. This can be illustrated by modifying the web-hosting example to make the ISP capture a proportion of the benefit produced by the materials posted on its servers. Consider again our web-hosting example but assume that, under the web-hosting agreement, the ISP is entitled to ten percent of the revenue derived by the subscriber from operating the site. In this modified example, the ISP does bear a cost, on the margin, for each item it decides to remove from its servers because any single item screened out by the ISP would reduce its expected revenue. The only remaining difficulty is that the loss suffered by the ISP is smaller than the actual loss borne by the subscriber. This problem, however, can be solved by scaling down the penalty imposed on the ISP. In our example, it can be easily shown that imposing a penalty of no more than 200 would induce the ISP to adopt the optimal monitoring technology, A.[95] Furthermore, as the analysis below regarding the liability of

---

94 My argument, it should be emphasized, is not that reducing penalties will have no effect on ISPs. Reducing penalties will reduce the magnitude of overdeterrence because ISPs will compare the magnitude of the penalty to their loss from losing subscribers. All that I argue is that reducing penalties cannot achieve *optimal* deterrence.

95 When the penalty equals 220, the ISP's expected costs under Technology A equal its expected costs under Technology B. Under Technology A, expected fees from posting an additional photograph are $10\% \times 200 \times (1 - 0.05) = 19$. Expected liability costs are $0.05 \times 200 = 10$, and the actual cost of monitoring is 20. The total value of Technology A is thus

auction sites will demonstrate,[96] the conditions under which reducing penalties would be optimal are not only a matter of theory. Rather, they would apply whenever the fees paid to the ISP are based on the profit-sharing model.

It should be noted, however, that combining strict liability with scaled-down penalties somewhat undermines the informational advantages of strict liability over negligence. To be sure, courts would not have to compare the ISP's actual monitoring policy with the socially optimal one. However, the institution setting the modified penalties—whether courts or legislators—would have to verify the socially optimal level of monitoring in order to deduce the necessary modifications in the magnitude of penalties.[97]

B. ISP-Subscriber Interface Regulation

As explained in Part II, the divergence of incentives between ISPs and their subscribers is the outcome of various impediments to the ability of the parties to contract on the optimal level of monitoring. The strategy outlined in this subpart seeks to alleviate overdeterrence by directly regulating the relationship between subscribers and ISPs to reduce their incentive divergence. This model of legal response does not exclude other legal strategies, and could be combined with other measures such as monitoring regulation to eliminate misconduct without producing overdeterrence.

Through regulation, lawmakers can impose uniform measures that will reduce the cost of transacting over monitoring policy and facilitate negotiation between service providers and their subscribers. For example, the law could require providers of web-hosting services to notify subscribers immediately whenever they decide to remove materials from their servers. Likewise, the law could require the providers of Internet access services to notify their users whenever they decide to block their access to a particular site. Such a notification requirement would have two potential effects. First, it would decrease the cost for subscribers of learning about such removal. As mentioned earlier, the lack of information about removal decisions by ISPs impedes the ability of the parties to alleviate privately the overdeterrence problem.[98] Also, expecting their censorship decisions to become immediately known to subscribers, ISPs might be less eager to remove materials from the Internet. Second, an immediate notifica-

---

$19 - 10 - 20 = -11$. Under Technology B, expected fees are $10\% \times 200 \times (1 - 0.06 - 0.09) = 17$. Expected liability costs are $0.04 \times 200 = 8$, and the actual cost of monitoring is 20. The total value of Technology B is thus $17 - 8 - 20 = -11$.

96 *See infra* Part IV.C.

97 In addition, the institution setting the penalties would have to obtain information about the fraction of the social loss borne by the ISP.

98 *See supra* Part II.A.2.

toring beyond the level set by the courts increases cost but does not reduce expected liability.[105]

3. *Regulation vs. Negligence*

Both monitoring-regulation and negligence-based regimes avoid overdeterrence by requiring ISPs to comply with an externally determined standard of monitoring.[106] The regimes differ, however, in the identity of the institution setting the required level of monitoring. Accordingly, the choice between regulation and negligence largely depends on the respective abilities of lawmakers and courts to determine *accurately* the optimal level of monitoring. While this Article does not advance a definitive position on the identity of the institution better positioned to identify the optimal level of monitoring, I would like to highlight several important considerations in determining whether negligence or regulation is most suitable in the ISP context, where rapid technological advancements constantly affect the optimal level of monitoring.[107]

In the short run, a monitoring-regulation regime provides greater certainty and thus decreases the likelihood of overdeterrence. As new technologies emerge, courts will struggle to set the optimal level of monitoring, and the likelihood of contradictory verdicts is substantial. Because ISPs would be imperfectly informed about what courts would determine to be the optimal level of monitoring, they would tend to reduce their exposure to liability by engaging in excessive monitoring policies. Conversely, explicitly specifying the optimal level of monitoring through regulation provides ISPs with superior information and reduces the risk of inconsistent verdicts. In the long run, in contrast, after the pace of technological change has slowed, industry standards are likely to emerge and courts are more likely to converge on the optimal level of monitoring even under a negligence standard.

---

105 However, once the assumption of full information is relaxed, negligence standards would result in overcompliance in a greater magnitude than would first-party negligence standards. On the tendency of negligence standards to overdeter under conditions of imperfect information, see Richard Craswell & John E. Calfee, *Deterrence and Uncertain Legal Standards*, 2 J.L. ECON. & ORG. 279, 279–80 (1986); and Louis Kaplow & Steven Shavell, *Accuracy in the Determination of Liability*, 37 J.L. & ECON. 1, 1–3 (1994). Given the divergence of incentives between ISPs and their users, this overdeterrence effect would be exacerbated with respect to ISPs, but would be minimized by employing negligence standards combined with reduced penalties.

106 Both regimes also differ from strict liability in their effect on the scale of services provided by ISPs. *See supra* Part I.B.

107 An additional consideration affecting the choice: regulations can be easily avoided when lawmakers fail to capture all relevant dimensions of care within the relevant regulation. For an analysis of the choice between legal rules and legal standards, see generally Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992).

On the other hand, the rapid pace of technological change might make negligence superior to regulation. When monitoring technologies constantly evolve, there is a risk that a standard set by lawmakers would become obsolete by the time it is applied by courts. Assigning the power to set monitoring standards to courts, by contrast, enables them to modify the optimal level of monitoring according to technological developments.[108]

4. *Knowledge-Contingent Standards*

I conclude the review of legal responses by discussing knowledge-contingent standards. Academics have often advocated knowledge-contingent standards as a response to overdeterrence.[109] However, although knowledge-contingent standards indeed avoid overdeterrence, they also encourage ISPs to ignore subscriber misconduct. Thus, knowledge-contingent standards should only be applied in conjunction with a monitoring-regulation regime.

Knowledge-contingent standards impose liability on ISPs only for their failure to remove materials they know to be illegal.[110] This would eliminate the overdeterrence problem simply by exempting ISPs from liability for their failure to acquire information about their users' conduct. Consider a regime under which the only duty imposed on ISPs is to remove materials that they know to be illegal. Under this strictly knowledge-contingent regime, ISPs have no reason to investigate the nature of the information disseminated through their networks, and the risk of excessive monitoring is eliminated. To be sure, some level of overdeterrence might persist if courts err in inferring knowledge, or if ISPs are too cautious in removing materials when they cannot determine with certainty that these materials are legitimate. Nevertheless, the magnitude of this overdeterrence phe-

---

108 *But see* Isaac Ehrlich & Richard A. Posner, *An Economic Analysis of Legal Rulemaking*, 3 J. LEGAL STUD. 257, 279 (1974) (describing common-law judicial process as too slow to keep up with the need for legal change resulting from growth in economic activity).

109 *See* Yen, *supra* note 14, at 1892 ("Whatever the wrongs embodied in copyright infringement, they are not serious enough to warrant ISP liability unless knowing assistance in that infringement is present."); *cf.* Ronald A. Cass & Keith N. Hylton, *Antitrust Intent*, 74 S. CAL. L. REV. 657, 680–81 (2001) (positing that intent standards are necessary to prevent both overdeterrence and underdeterrence in the antitrust context). In his gatekeeper paper, Kraakman discussed the role of scienter standards in third-party liability. *See* Kraakman, *supra* note 27, at 76; *see also* Jackson, *supra* note 33, at 1057 (exploring the role of knowledge standards in governing the liability of lawyers for the misconduct of their clients).

110 This is usually achieved by imposing liability only on ISPs that "knowingly" failed to take the necessary steps to prevent misconduct. The DMCA, for example, precludes monetary liability of hosting-services providers that have no knowledge of subscriber infringement. *See* 17 U.S.C. § 512(c)(3)(B) (Supp. V 1999).

tion requirement would facilitate ex post negotiation between the parties over the fate of particular items. For example, once notified about such removal, a subscriber who believed that an item was legal could convey information about the legal status of the item to the ISP.

The most prominent statute governing ISP liability, the Digital Millennium Copyright Act (DMCA),[99] has partially adopted the regulation model suggested by this section. The DMCA provides an elaborate set of regulations affecting the cost of contracting over censorship practices between ISPs and their subscribers and regulates the level of policing by ISPs.[100] However, as will be explained below,[101] the DMCA has not gone far enough in alleviating the impediments to contracting.

C. Monitoring Standards

The conventional endorsement of strict liability is premised on the recognition that wrongdoers are best positioned to determine the optimal level of care because they capture both social harm and social benefit. Part I has shown that this premise does not apply to ISPs. The strategy explored in this subpart renders the divergence of incentives between ISPs and their subscribers irrelevant for ISP monitoring decisions by granting the state the power to set the required level of ISP monitoring. This strategy can take two doctrinal forms: monitoring-regulation and negligence-based standards.

1. *Monitoring Regulation*

A monitoring-regulation regime assigns lawmakers, rather than ISPs, the task of setting the optimal level of monitoring. This regime would impose liability on ISPs for user misconduct only when they failed to meet monitoring standards set by regulators.[102] An ISP that satisfies the level of monitoring set by lawmakers will not be liable for the misconduct of its subscribers.

A monitoring-regulation regime eliminates overdeterrence by making the divergence of incentives between ISPs and their subscribers irrelevant for ISPs' decision to monitor. This is because the

---

99 17 U.S.C. § 512 (Supp. V 1999).

100 *See id.*

101 For a discussion of the interface-regulation aspects of the DMCA, see *infra* Part IV.B.

102 A monitoring-regulation regime might also impose penalties for failure to meet monitoring standards in the absence of harm. The rules governing the sale of alcohol to minors serve as a good example for such regimes. Sellers must ask for identification before each sale of alcohol. Failure to ask for age documents will result in penalties even if the customer turns out to be an adult. For a general analysis of the choice between liability for harm versus ex ante regulation, see Steven Shavell, *Liability for Harm Versus Regulation of Safety*, 13 J. LEGAL STUD. 357 (1984).

calculus of ISPs under this regime differs from their calculus under strict liability. Under strict liability, ISPs would have to identify the optimal level of monitoring by comparing the full social harm produced by subscriber misconduct to the cost of monitoring and the loss produced by screening out materials. In contrast, under a monitoring-regulation regime, ISPs would compare the cost of complying with the regulation with the expected liability for failure to comply. An ISP would have no incentives to monitor beyond the level specified by lawmakers because the marginal increase in monitoring cost would exceed the marginal saving in liability costs.[103]

A monitoring-regulation regime requires lawmakers to acquire information not only about the social harm of user misconduct, but also about the actual cost of monitoring, its effectiveness in detecting misconduct, and its effect on legitimate conduct. To be sure, legislators are likely to err in setting the optimal level of monitoring. But as long as they are better positioned than ISPs to determine that level, regulation is superior to strict ISP liability.

2. *Negligence*

Negligence-based standards serve as the traditional remedy for overdeterrence problems associated with "positive externalities."[104] Under a negligence regime of ISP liability, the optimal level of monitoring would be specified by courts, so that service providers will be held liable for the misconduct of their subscribers only if they fail to meet that standard. An ISP whose actual monitoring policies equal, or exceed, the level set by the courts will be exempted from liability.

Like the monitoring-regulation regime, a negligence-based approach does not rely on defendants to calculate the optimal level of monitoring. Instead, courts will determine the optimal level of monitoring by taking into account the social harm produced by user misconduct, the actual cost of monitoring, its effectiveness in detecting misconduct, and its effect on legitimate conduct. If courts succeed in specifying the socially desirable level of monitoring, ISPs will have no incentive to monitor excessively because increasing the level of moni-

---

103 Similarly, ISPs would have no incentive to adopt suboptimal monitoring policies because the expected liability resulting from failure to satisfy regulatory monitoring requirements would exceed the savings in monitoring costs.

104 *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 729–37 (5th ed. Aspen Publishers, Inc. 1998) (endorsing the adoption of negligence standards for libel, among other harmful forms of speech, because of the external benefits of speech); Hylton, *supra* note 58, at 984 (positing that when external benefits are present, "[a] negligence rule, which would not internalize all victim losses, may be socially preferable precisely because it fails to have the same taxing effect on the activity level as would a strict liability rule"); Katyal, *supra* note 4, at 1095–1101 (advocating the use of negligence standards to cope with the risk of overdeterrence produced by network effects).

nomenon will most likely be smaller than its magnitude under strict liability.[111]

One might argue that even a regime based purely on knowledge standards would fail to eliminate the overdeterrence problem. The analysis so far has focused on the effect of third-party liability on the level of *monitoring* by the ISP. In theory, however, the divergence of incentives associated with the third party–primary wrongdoer relationship could lead to overdeterrence even under conditions of full information. Consider again the web-hosting example, and assume that there is no doubt that a given statement posted on the site is false and thus libelous. The website owner would remove such a statement from her site only if the expected harm of libel exceeded her expected benefits from posting the statement. The ISP, by contrast, does not take the benefits produced by posting the statement into account, and thus might remove the statement, even if its value exceeds the cost of libelous publication.

This argument is valid, however, only under the assumption that the value that the subscriber derives from posting statements on the Internet is distributed across false statements in the following way. If the value of posting some libelous statements exceeds the social harm associated with libel, and the value of posting other libelous statements is clearly outweighed by the cost of libel, then conventional economic theory suggests that the use of penalties equal to social harm would induce wrongdoers to post statements of the former type and remove statements of the latter type. However, because the third party, the ISP, does not capture the full value of the conduct at stake, making it pay for the full social harm would result in overdeterrence, even under a regime based on knowledge standards.

In most instances of online misconduct, however, the conduct at stake seems to be strictly undesirable under conditions of full information; that is, the benefit derived from the conduct is always lower than the resulting social harm. For example, it is difficult to imagine circumstances under which the social benefit of a clearly false statement exceeds the harm produced by its publication. Hence, the ISP overdeterrence effect would most likely be limited to the monitoring policies adopted by ISPs, and the ensuing amount of true statements removed from the Internet. Stated differently, there is no concern of overdeterrence with respect to materials known to be illegal.

---

111 This problem could also be solved through the adoption of a narrow formulation of the governing "knowledge" standard. *See* Yen, *supra* note 14, at 1877 ("If either [a formally filed] complaint or [an ISP's subsequent] investigation reveals a 'colorable' claim of noninfringement, the ISP need not worry about contributory liability because the required knowledge does not exist.").

At the same time, however, the advantage of knowledge-contingent standards of third-party liability, their elimination of monitoring incentives, is also their major flaw. Knowledge-contingent standards not only eliminate incentives to monitor, but also create incentives for ISPs to maintain their ignorance to minimize their liability exposure.[112] An optimal regime of ISP liability should thus combine knowledge-contingent and monitoring-regulation standards. To illustrate, consider the liability of web-hosting service providers for a defamatory statement posted on a subscriber's site. Under such a combined regime, the ISPs would be subjected to regulations specifying the extent to which they should monitor their servers to determine whether the materials posted by subscribers are defamatory. An ISP's failure to satisfy the monitoring requirements set forth in the regulations will expose it to liability for libel. These monitoring regulations would be supplemented with a rule under which an ISP would be liable for libel whenever it knew about a defamatory statement and failed to remove it from its servers. The interaction of knowledge-contingent standards and a monitoring-regulation regime would therefore lead to optimal deterrence.

IV
APPLICATIONS

The framework developed in the preceding Parts provides illuminating insights about intriguing features of third-party liability regimes outside the Internet context. Examples include the three-tiered regime of liability for libel,[113] the distinction between producers and distributors of child pornography,[114] and employer liability

112 *See, e.g.*, Matt Richtel, *EBay Says Law Discourages Auction Monitoring*, N.Y. TIMES, Dec. 10, 1999 (reporting that eBay deliberately avoids screening auctions before they appear online to avoid knowledge-contingent liability under the DMCA), *at* http://www.nytimes.com/library/tech/99/12/cyber/articles/10ebay.html. The perverse incentives to acquire information produced by knowledge-contingent standards are well recognized by the literature on mistake of law as a criminal defense. *See, e.g.*, Sharon L. Davies, *The Jurisprudence of Willfulness: An Evolving Theory of Excusable Ignorance*, 48 DUKE L.J. 341, 385 (1998) ("The inevitable drawback of any rule excusing criminal liability for a lack of knowledge of the law is that such a rule celebrates ignorance of the law while making knowledge of it the best and fastest ticket to a prison cell.").

113 The common law of defamation distinguishes between three types of defendants. "Common carriers" (such as telephone companies) are not liable for defamation. "Distributors" of published material, such as bookstore owners, are liable only when they have actual knowledge of the defaming nature of the publication. "Publishers," by contrast, will be held liable for defamation regardless of their state of mind. *See, e.g.*, Waldman, *supra* note 26, ¶ 33.

114 *See, e.g.*, United States v. X-Citement Video, Inc., 513 U.S. 64, 67–78 (1994) (interpreting the relevant statute to require knowledge of minority status by child pornography distributor in order to avoid constitutional challenges); Gilmour v. Rogerson, 117 F.3d 368, 372–73 (8th Cir. 1997) (imposing strict liability on a producer of sexually explicit materials depicting minors).

for sexual harassment.[115] Broader implications notwithstanding, this Part utilizes the incentive-divergence thesis to shed light on three specific aspects of third-party liability in cyberspace. First, I show how recognizing the incentive-divergence problem illuminates the complex doctrine of vicarious copyright infringement, and explains its role in the *Napster* decisions. Next, I evaluate the regime of ISP liability under the Digital Millennium Copyright Act.[116] Finally, I outline the desirable liability regime for auction sites.

The discussion below does not seek to cover all instances of third-party liability in cyberspace.[117] Indeed, the thesis underlying this Article is that no single regime could be crafted to cope with all types of subscriber misconduct. Rather, an optimal regime of ISP liability should be tailored according to the nature of the service at stake and the type of subscriber misconduct involved. As Part II has shown, the nature of the service offered by the ISP affects the degree to which the parties can contractually overcome their divergence of incentives. The type of subscriber misconduct in turn dictates the ability of the ISP effectively to detect unlawful conduct by its subscribers.[118] Given the difficulty of devising a single regime of ISP liability, my goal in this Part is to merely illustrate the illuminative implications of the incentive-divergence thesis for understanding current doctrine, and designing optimal regimes, of ISP liability.

---

115 *See generally* Balkin, *supra* note 85 (discussing sexual harassment in the workplace); Eugene Volokh, *Freedom of Speech, Cyberspace, Harassment Law, and the Clinton Administration*, LAW & CONTEMP. PROBS., Winter/Spring 2000, at 299 (discussing sexual harassment effected through the Internet).

116 17 U.S.C. § 512 (Supp. V 1999).

117 The list of subscriber misconducts for which ISPs might be liable continues to expand. *See, e.g.*, Lonn Weissblum, Comment, *Incitement to Violence on the World Wide Web: Can Web Publishers Seek First Amendment Refuge?*, 6 MICH. TELECOMM. & TECH. L. REV. 35, 52–57 (2000) (analyzing civil and criminal liability of websites publishing instructions for bomb making).

118 As mentioned above, extending liability to ISPs is justified only under the assumption that they are positioned to prevent subscriber misconduct at a relatively low cost. *See supra* text accompanying notes 33–36. To illustrate the interaction of the nature of the misconduct and monitoring costs, consider the difference between defamation and hate speech. An operator of online chat rooms can relatively easily detect most messages containing hateful content through a basic textual search. On the phenomenon of online hate, see Lisa Guernsey, *Mainstream Sites Serve as Portals to Hate*, N.Y. TIMES, Nov. 30, 2000, at G1. In contrast, as the sheer reading of a message cannot reveal whether it is true or false, the cost of detecting a defaming message by the operator of online chat rooms might be prohibitive. Legal context also determines other important aspects, such as the optimal role of victim care in preventing subscriber misconduct. For a discussion of the role of victim care in the prevention of copyright infringement, see *infra* text accompanying notes 186–87.

A. Vicarious Infringement: A New Approach

The doctrine of vicarious copyright infringement, which has occupied a key role in the attempts of content providers to hold ISPs liable for subscriber copyright infringement,[119] is in disarray. The conflicting interpretations of this doctrine are best illustrated by the diametrically opposed positions of the Ninth Circuit and the district court in the *Napster* case regarding the scope of Napster's vicarious liability for copyright infringement.[120] In this subpart, I uncover a new rationale underlying this important doctrine.[121] This new understanding, I believe, will enable courts to apply the vicarious infringement doctrine to ISPs in a principled, coherent manner.

Under the commonly accepted rationale, the goal of vicarious infringement is to go beyond the technical definitions of direct copyright infringement and identify the party that should internalize the social cost of infringement. In this section, however, I suggest an alternative rationale for vicarious infringement. Under this new understanding, an alternative objective of vicarious infringement is to provide third parties with incentives to police infringement while eliminating the risk of overdeterrence due to the divergence of incentives between primary wrongdoers and third parties. While the current rationale might account for the contours of vicarious infringement in many other contexts, it is this new rationale that should inform the application of the doctrine to ISPs.

---

119 For a review of pre-*Napster* decisions struggling with the application of vicarious liability to ISPs, see Yen, *supra* note 14, at 1843–48. The doctrine of vicarious liability continues to occupy an important role in the post-*Napster* era. For example, in a recent complaint, members of the music and movie industries argue that several companies operating peer-to-peer file-trading services vicariously infringe their copyrights. *See* Complaint for Damages and Injunctive Relief for Copyright Infringement, MGM Studios Inc. v. Grokster, Ltd., No. 01-08541 (C.D. Cal. filed Oct. 2, 2001), *available at* http://cyber.law.harvard.edu/seminar/internet-client/readings/week8/complaint.pdf; Lee Gomes, *Entertainment Industry Sues to Curtail Web Music-Sharing Morpheus*, WALL ST. J., Oct. 4, 2001, at B9.

120 *See* A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001), *aff'g in part and rev'g in part* 114 F. Supp. 2d 896 (N.D. Cal. 2000). The *Napster* decision raises siguificant questions over the future of digital music and the proper scope of intellectual property protections. In this Article, however, I abstract from these substantive issues and analyze the methods of enforcement employed by the courts under the assumption that Napster's users commit infringement when they use the service. For scholarship on the implications of the case for digital distribution of music, see Raymond Shih Ray Ku, *The Creative Destruction of Copyright:* Napster *and the New Economics of Digital Technology*, 69 U. CHI. L. REV. (forthcoming 2002); and Alfred C. Yen, *A Preliminary Economic Analysis of* Napster*: Internet Technology, Copyright Liability, and the Possibility of Coasean Bargaining*, 26 U. DAYTON L. REV. 247, 263–76 (2001).

121 Traditional doctrines of copyright enforcement maintain their importance despite the enactment of the DMCA. First, for example, although the DMCA provides ISPs with safe havens from liability, an ISP that fails to qualify for such immunity will have its liability determined by the traditional rules of copyright liability. *See* 17 U.S.C. § 512(c) (Supp. V. 1999). Second, the DMCA's definition of "service provider" does not cover all types of Internet services. *See* § 512(k)(1).

1. *The Legal Landscape: Broad vs. Narrow Approach*

Napster provided its subscribers with the ability to locate and share MP3 files.[122] A full description of the Napster system is beyond the scope of this Article.[123] For our purposes, it is sufficient to note that Napster did not store the relevant MP3 files on its servers.[124] Rather, it maintained a list containing the names of MP3 files available for downloading at any given time, and the Internet Protocol (IP) addresses from which they could be downloaded.[125]

Several major record companies sued Napster on the grounds that its service constitutes vicarious (and contributory) infringement of their copyrighted music.[126] Both the district court and the Ninth Circuit issued a preliminary injunction enjoining Napster from facilitating the downloading of copyrighted music through its servers.[127] These courts, however, held different positions with regard to the scope of this injunction. The district court refused to examine Napster's argument that it is implausible to distinguish legal and nonlegal downloads, and ruled that Napster must screen out *all* infringing files on its server, regardless of its ability to identify them as infringing.[128] The Ninth Circuit remanded and instructed the district court to issue a new injunction.[129] The new injunction, held the Ninth Circuit, would have to take into consideration the limited ability of Napster to distinguish infringing and non-infringing files given the architecture of its system.[130] Concretely, the Ninth Circuit noted that Napster does not store the files on its servers and therefore it is able to detect infringement based only on the names given by subscribers to the files they offer for downloading.[131] Thus, Napster incurs liability for infringement only if copyright holders provide Napster with notices of infringing files that the ISP does not then remove.[132]

---

122 *Napster, Inc.*, 239 F.3d at 1011.

123 For such a description, see Ariel Berschadsky, RIAA v. Napster: *A Window onto the Future of Copyright Law in the Internet Age*, 18 J. MARSHALL J. COMPUTER & INFO. L. 755, 759–62 (2000).

124 *Napster, Inc.*, 239 F.3d at 1011–13.

125 *Id.* at 1012.

126 *Id.* at 1010–11; A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 900 (N.D. Cal. 2000).

127 *See Napster, Inc.*, 239 F.3d at 1029; *Napster, Inc.*, 114 F. Supp. 2d at 927.

128 *Napster, Inc.*, 114 F. Supp. 2d at 926–27.

129 *Napster, Inc.*, 239 F.2d at 1029.

130 *See id.* at 1023–24 (noting that the district court failed to recognize that Napster's ability to control subscriber infringement is "cabined by the system's current architecture").

131 *See id.* at 1024 (stating that "the file name indices . . . are within the 'premises' that Napster has the ability to police").

132 *See id.* at 1027. The district court then issued a new injunction based on the instructions of the Ninth Circuit. *See* A & M Records, Inc. v. Napster, Inc., Nos. C 99-05183 MHP, C 00-1369 MHP, 2001 WL 227083 (N.D. Cal. Mar. 5, 2001). As of March 15, 2001, prelimi-

The opposing views expressed by these courts echo an old dispute over the proper boundaries of vicarious infringement. Copyright law recognizes three avenues for holding a party liable for copyright infringement: direct, contributory, and vicarious liability. Direct infringement occurs when a party makes a copy of the copyrighted work, i.e., exercises one of the copyright owner's exclusive rights without permission.[133] Making unauthorized copies of a music CD for commercial purposes would constitute a paradigmatic example of direct infringement. The standard governing direct infringement is strict liability, so that neither knowledge nor intent is required to find a party liable under this doctrine.[134]

Despite statutory silence regarding third-party liability,[135] courts have recognized two types of third-party liability for copyright infringement—contributory and vicarious liability. To establish contributory liability, two conditions must be satisfied: (1) the third party must cause or contribute to the infringing activity;[136] and (2) the third party must know or have reason to know about the primary wrongdoer's infringing conduct.[137] Examples of contributory liability include the furnishing of infringing videotapes to another for purposes

---

nary reports indicted that Napster has blocked the exchange of more than one-half of the files. John Borland, *Napster Filters More than Half of Downloads*, CNET NEWS.COM, Mar. 15, 2001, *at* http://news.cnet.com/news/0-1005-200-5149337.html. At the time that this Article was submitted for publication, the parties were still litigating over the proper scope of the preliminary injunction and the extent to which Napster complies with its requirements. *See* Matt Richtel, *Napster Appeals an Order to Remain Closed Down*, N.Y. TIMES, July 13, 2001, at C4; Matt Richtel, *Napster Wins a Stay*, N.Y. TIMES, July 19, 2001, at C4 (reporting recent developments in this dispute).

133 17 U.S.C. § 106 (1994 & Supp. V 1999) (listing the exclusive rights of copyright owners); *id.* § 501(a) (Supp. V 1999) (stating that infringement occurs when alleged infringer violates at least one of the exclusive rights granted to copyright holders).

134 *See* 4 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 13.08 (2001) (explaining that good-faith mistakes and ignorance do not constitute defenses to a finding of direct infringement, though they might affect remedies).

135 The Supreme Court noted that the lack of specific reference to secondary liability within the Copyright Act does not preclude the imposition of liability on third parties. *See* Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 435 (1984).

136 *See* Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) (defining a contributing party as "one who . . . induces, causes or materially contributes to the infringing conduct of another"); *see also* Matthew Bender & Co. v. West Publ'g Co., 158 F.3d 693, 706 (2d Cir. 1998) (explaining that a party may incur contributory liability if he engages in "personal conduct that encourages or assists the infringement").

137 *Gershwin Publ'g Corp.*, 443 F.2d at 1162. Several decisions have imposed contributory liability if the third party *should* have known about the infringing conduct. *See* Cable/Home Comm. Corp. v. Network Prods., Inc., 902 F.2d 829, 845 & n.29 (11th Cir. 1990) (requiring that the secondary infringer "know or have reason to know" of the infringement); Religious Tech. Ctr. v. Netcom On-Line Comm. Servs., 907 F. Supp. 1361, 1374 (N.D. Cal. 1995) (framing issue as "whether Netcom knew or should have known" of infringing activities).

of public performance, and the distribution by individual *A* of unauthorized copies made by individual *B*.[138]

Establishing vicarious liability requires the satisfaction of a two-pronged test: (1) the defendant must have had the *right and ability to supervise* the misappropriation of the copyrighted work; and (2) the defendant must have had a *direct financial interest* in the exploitation of the copyrighted material.[139] Unlike vicarious liability in torts, vicarious liability for copyright infringement extends beyond the employer-employee relationship. Moreover, whereas contributory infringement requires defendants to be aware of the infringement, defendants that satisfy the requirements for vicarious liability are liable regardless of their degree of awareness of the infringing conduct.[140]

While the scope of direct liability is relatively clear,[141] the distinction between vicarious and contributory liability is often a matter of dispute and a subject of litigation.[142] The controversy has focused on the interpretation of the ability-to-supervise prong of vicarious liability, also known as the "control" requirement.[143] Two competing approaches have emerged regarding the requisite degree of third-party

---

138 *E.g.*, Encyclopedia Britannica Educ. Corp. v. C.N. Crooks, 558 F. Supp. 1247, 1249, 1256 (W.D.N.Y. 1983) (supplying infringing tapes); Prather v. Camerarts Publ'g Co., 1972 WL 17668 (N.D. Ill. Apr. 19, 1972) (distribution).

139 *See* Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963). The Second Circuit explained:

> When the right and ability to supervise coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials—even in the absence of actual knowledge that the copyright monopoly is being impaired—the purposes of copyright law may be best effectuated by the imposition of liability upon the beneficiary of that exploitation.

Id. (citations omitted).

140 *See* 3 NIMMER & NIMMER, *supra* note 134, § 12.04[A][1] (noting that "[l]ack of knowledge that the primary actor is actually engaged in infringing conduct is not a defense" under the doctrine of vicarious infringement).

141 The Internet context, however, demonstrates that the traditional definition of direct liability may not be appropriate for cyberspace. *See, e.g.*, Playboy Enters. v. Frena, 839 F. Supp. 1552, 1554–59 (M.D. Fla. 1993) (finding that the operator of a bulletin board service directly infringed the copyrights of *Playboy* magazine by allowing users to upload illegal copies of *Playboy*'s photographs), *superseded by statute as stated in* ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619 (4th Cir. 2001); *see also* Jennifer E. Markiewicz, *Seeking Shelter from the MP3 Storm: How Far Does the Digital Millennium Copyright Act Online Service Provider Liability Limitation Reach?*, 7 COMMLAW CONSPECTUS 423, 430–31 (1999) (describing courts' shift from direct to secondary liability for ISPs based on the recognition that traditional methods of analysis are not appropriate).

142 The distinction is of significant practical importance due to the difference in the level of knowledge about the infringing activity required by each category. Whereas contributory liability requires some degree of awareness of primary infringement, vicarious liability is imposed regardless of the third party's state of mind concerning the primary infringement. *See supra* text accompanying notes 137, 140.

143 *See* Charles S. Wright, *Actual Versus Legal Control: Reading Vicarious Liability for Copyright Infringement into the Digital Millennium Copyright Act of 1998*, 75 WASH. L. REV. 1005, 1012–20 (2000) (reviewing the conflicting approaches on the scope of the control prong of vicarious liability for copyright infringement).

control over the infringement by the primary wrongdoer: the "broad" approach and the "narrow" approach.[144]

a. *Legal Control*

The broad view extends liability to a party based on its "legal," or potential, power to control the infringing conduct.[145] This approach therefore finds control in any relationship in which the third party reserves to itself, in principle, control over the infringing conduct even when effectively exercising such control to distinguish between infringing and non-infringing conduct, and to prevent only the former, is impractical.[146] For example, it has been determined that a finding of control of a trade show organizer over unauthorized uses of songs by booth operators would be justified because the defendant had the right to veto the playing of any music at all, even though he lacked the ability to distinguish between authorized and unauthorized songs.[147] Phrased differently, the broad approach to the control requirement assigns no weight to the cost of acquiring information about the infringing nature of the activity. Rather, it finds control whenever the third party, assuming that it knows of the nature of the conduct, can prevent it from taking place. By focusing on Napster's alleged inability to distinguish infringing and non-infringing files exchanged through its servers, the district court evidently endorsed this broad approach to the control requirement.

b. *Actual Control*

The narrow approach, in contrast, requires third parties to be practically able to distinguish infringing and non-infringing conduct in order to be liable for vicarious infringement. Under this approach, "control requires more than the potential right to cease all activities undifferentiated from the infringement, the right to terminate other activities, or the effective ability to terminate only after infringement is evident."[148] Instead, it requires that the third party could take "meaningful steps to prevent infringement."[149] Stated differently, the narrow approach requires not only that the cost of preventing conduct known to be infringing be low, but also that the cost of monitoring

144 *Id.*

145 *Id.* at 1016–18.

146 *See* Kirkwood, *supra* note 51, at 719.

147 *See* Polygram Int'l Publ'g, Inc. v. Nevada/TIG, Inc., 855 F. Supp. 1314, 1325–26, 1328–29 (D. Mass. 1994). The Second Circuit adopted similar logic in the *Gershwin* case, in which it found that the defendant, an organizer of a circuit of community concerts, had satisfied the "control" requirement merely because the relevant contract placed the defendant "in a position to police the infringing conduct of its artists." Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1163 (2d Cir. 1971).

148 Wright, *supra* note 143, at 1013 (footnote omitted).

149 *Id.*

conduct of primary wrongdoers to determine whether it is infringing will be low.[150] This approach is best illustrated by the position adopted by the Ninth Circuit in *Napster*. As described earlier, this court ruled that the injunction must take into account Napster's ability to identify infringing files.

c. *Implications for ISP Liability*

As evidenced by the *Napster* litigation, the choice between these two approaches has significant implications for ISPs. ISPs undoubtedly have full technical control over subscribers' conduct, whether infringing or not. Hosting service providers, for example, are technically positioned to remove all subscribers' information stored on their servers.[151] Accordingly, they would nearly always satisfy the control requirement of vicarious infringement under the broad approach. Adopting the broad approach would therefore render most ISPs vicariously liable for subscriber copyright infringement, and therefore would subject ISPs to liability even when they were clearly unable to distinguish between legitimate and unlawful subscriber conduct. Put differently, adopting the broad approach would impose an effective regime of strict ISP liability for subscriber misconduct. Under the narrow approach, in contrast, ISPs would be liable only for the misconduct that they were capable of detecting.

The risk of imposing strict liability on ISPs based exclusively on their technical ability to control user misconduct has sparked academic writing vigorously objecting to the adoption of the broad version of the control requirement with respect to ISPs.[152] Before discussing which test should apply to ISPs, I shall now explore the conventional economic understanding of vicarious infringement and offer a new understanding that would illuminate the proper application of vicarious liability to ISPs.

2. *A New Rationale for Vicarious Infringement*

Under its predominant explanation, vicarious infringement aims at identifying the real primary wrongdoer. That is, its objective is to go beyond the narrow, technical definition of direct infringement to identify a broader set of parties who should ultimately internalize the

---

150 *See* Artists Music, Inc. v. Reed Publ'g (USA), Inc., Nos. 93 CIV. 3428 (JFK), 73163, 1994 WL 191643, at *6 (S.D.N.Y. May 17, 1994) (explicitly considering the prohibitive supervision cost by a trade show organizer with respect to music played by exhibitors, and refusing to find "control"); Wright, *supra* note 143, at 1014 (stating that "[t]he cost of policing can also preclude a finding of actual control").

151 Note also that most ISPs reserve for themselves, in their agreement with their users, the right to remove materials, and thus satisfy the "legal right" element of the control test.

152 *See, e.g.*, Elkin-Koren, *supra* note 49, at 399–410; Wright, *supra* note 143, at 1026–36; Yen, *supra* note 14, at 1843–72.

cost of infringement.[153] Consider the paradigmatic example of vicarious liability in copyright—the liability of dance hall proprietors for copyright violations by musicians that they hire to perform on their property.[154] Under this predominant understanding, dance hall proprietors are held strictly liable because they should internalize the cost of infringement notwithstanding the direct infringement by the musicians they hire.

This economic rationale for vicarious infringement justifies the broad interpretation of the control element. Under economic theory, primary wrongdoers should internalize the cost of their misconduct regardless of their ability to prevent it. All that matters is that the defendant is one who should scale its level of activity to the socially desirable level taking into account the costs of its misconduct. Thus, the "ability and control" element of vicarious infringement should not be limited to parties who can effectively police infringement and accurately distinguish infringing and non-infringing uses. Rather, it should be desigued to identify parties who should bear the cost of infringement even when avoiding infringement is too costly.[155]

I believe, however, that identifying primary wrongdoers might not be the only economic objective underlying vicarious infringement. An alternative objective of vicarious infringement might be to impose liability on *third parties* while eliminating the risk of overdeterrence produced by the divergent incentives of primary infringers and third parties. As I shall demonstrate below, recognizing this alternative rationale has important implications for ISP liability.

As explained in Part I, an optimal regime of third-party liability should target only parties who are positioned to prevent inexpensively the misconduct at stake.[156] Contributory infringement targets one class of parties who are in such a position by penalizing those who know about the infringement. However, limiting liability to informed third parties leaves out those who, although initially uninformed, can monitor and detect infringement at a relatively low cost. Under its

153 *See* 3 NIMMER & NIMMER, *supra* note 134, § 12.04[A][1] (noting views under which the doctrine of vicarious infringement is "an application of the principle that a master is civilly liable for the wrongful acts of his servant performed within the scope of his employment, even if such acts are done without express authority or contrary to orders"); Yen, *supra* note 14, at 1843 (asserting that both vicarious infringement and the tort doctrine of respondeat superior "share a common basis in enterprise liability, which states that enterprises should internalize losses caused by their existence as a cost of doing business").

154 *See, e.g.*, Famous Music Corp. v. Bay State Harness Horse Racing & Breeding Ass'n, 554 F.2d 1213, 1214–15 (1st Cir. 1977) (holding racetrack vicariously liable for hiring infringer to play music to patrons).

155 Unfortunately, economic theory has yet to develop clear causation tests to distinguish primary and secondary wrongdoers. *See* discussion *supra* Part I.A.2 (reviewing the murky boundaries of the optimal-production objective).

156 *See supra* notes 32–33 and accompanying text.

alternative economic interpretation, the doctrine of vicarious infringement fills this gap by targeting third parties with low monitoring costs, and providing them with incentives to detect infringements.

This interpretation leaves an intriguing feature of vicarious infringement unexplained. Vicarious infringement requires that third parties derive financial gain from the underlying misconduct.[157] If liability is expanded to third parties based on their low costs of prevention, however, there seems to be no justification for further inquiring about the financial gains they derive from the infringing activity. After all, all courts need to do is apply the actual control test and determine whether the defendant has the effective ability to identify infringement.

At this juncture, the incentive-divergence thesis becomes relevant. As I have argued, imposing strict liability on third parties will induce them to monitor excessively. I have also shown that, the overdeterrence phenomenon notwithstanding, ISPs who capture a benefit for any additional item posted on their network are better positioned to self-assess the cost and the benefits of monitoring than other third parties.[158] The financial gain requirement can thus be interpreted as a mechanism to ensure that the third party captures at least a portion of the benefits of the conduct it is entrusted with policing. Under this interpretation, the financial gain requirement seeks to ensure that third parties, though positioned to monitor against infringements, will not engage in excessive monitoring because they do not internalize the social cost of their monitoring activities.

This new economic understanding of vicarious infringement has two implications for the requisite elements of vicarious infringement. First, because vicarious liability should be imposed on parties who can monitor effectively for copyright violations, courts should apply the narrow approach to the control requirement. Second, courts should construe the financial gain requirement narrowly, and refuse to rely on some vague, speculative link between defendants' profits and the infringing activity. Rather, the financial gain requirement should be satisfied only when the third party captures direct benefits from the conduct of the primary wrongdoer.[159]

To summarize, vicarious infringement serves two distinct functions: identifying *primary* infringers, and providing *third parties* with incentives to detect infringement. These different functions entail

---

157 *See* Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 307 (2d Cir. 1963).

158 *See* discussion *supra* Part III.A.

159 *Cf.* Ginsburg, *supra* note 15, at 1494 (arguing for vicarious, perhaps even direct, liability for commercial online service providers as they have "direct financial interest," particularly when "the availability of copyrighted works on the network enhances the service's appeal to potential subscribers").

different requirements for finding vicarious liability. While the first requires us to determine whether the particular defendant ought to internalize the losses from infringement, the second requires us to identify parties that are positioned to monitor copyright violations and that have interests which are somewhat aligned with those of primary infringers. The new economic objective that I offer is intended to supplement, rather than replace, the conventional understanding of vicarious infringement. To be sure, the distinct goals of vicarious infringement should be clarified, perhaps by creating two separate legal doctrines. Yet, even under the current legal regime, the new understanding of vicarious infringement can provide a framework for a sensible application of vicarious infringement to the providers of Internet services.

3. *ISPs:* Napster *Revisited*

Having identified an alternative economic function of vicarious infringement, I now turn to examine its implications for ISP liability.

As mentioned earlier, ISPs undoubtedly satisfy the broad version of the control requirement of vicarious infringement. However, for those who seriously believe that ISPs should not be perceived as primary wrongdoers, subjecting them to vicarious infringement is conceptually inconsistent with the traditional economic function of vicarious infringement. After all, if ISPs should not internalize the social loss produced by subscriber misconduct, why subject them to liability under a doctrine essentially aimed at primary wrongdoers?

The new understanding of vicarious liability fundamentally alters this picture. Because vicarious liability is also designed to target third parties capable of preventing infringement, there is no inconsistency in subjecting ISPs to vicarious infringement using the narrow version of the control requirement. Applying the narrow test of control will identify ISPs that are positioned to detect infringing conduct by subscribers. Imposing strict liability on these ISPs will provide them with incentives to police user conduct. By limiting liability to ISPs that derive some financial gains from items transmitted through their networks, vicarious infringement is less likely to result in excessive monitoring and overly stringent screening policies.

Finally, uncovering the distinct economic functions that underlie vicarious infringement sheds a new light on the positions of the district court and the Ninth Circuit in *Napster*. In adopting the broad version of the control requirement, the district court implied that Napster should ultimately internalize the social loss produced by its service. That is, according to the district court, Napster is a primary wrongdoer rather than a third party harnessed by the legal system to prevent wrongdoing by others. In contrast, the Ninth Circuit views

Napster as a third party. As a third party, Napster's scope of liability should be closely related to its ability to detect wrongdoing and prevent it. Thus, under the Ninth Circuit's logic, the scope of liability imposed on Napster should be determined by the practical ability of Napster, given the architecture of its service, to detect copyright infringement. Furthermore, as Napster was found to derive sufficient financial interest, subjecting it to vicarious liability is less likely to result in excessive blocking of files.

The discussion thus far has largely assumed the existence of the financial-interest element of vicarious liability. As mentioned above, this element of vicarious infringement is important in light of the divergence of incentives between ISPs and their subscribers, which could result in overdeterrence. For strict liability not to result in excessive monitoring and overzealous removal policies, the financial-interest element should be construed narrowly. Specifically, financial interest should be found only when the ISP bears an actual cost when censoring items stored on, or transmitted through, its networks. In the *Religious Center* decision, for example, the district court ruled that a provider of web-hosting services for online bulletin board services does not meet the financial benefit requirement because it charges fiat fees for its service.[160] In the *Napster* case, the district and circuit courts found financial interest based on Napster's future plans to charge fees for its service.[161] The commercial use of the Internet is still in its early stages, and Internet business models are evolving at a rapid pace.[162] Thus, it seems courts must continue to struggle with the precise nature of the financial-gain requirement under the narrow interpretation of vicarious infringement.

B. The Digital Millennium Copyright Act

This subpart will assess the success of Title II of the Digital Millennium Copyright Act of 1998 (DMCA),[163] the most extensive regula-

160 Religious Tech. Ctr. v. Netcom On-Line Comm. Servs., 907 F. Supp. 1361, 1376–77 (N.D. Cal. 1995) (noting, nonetheless, that the provider potentially did have the ability to supervise); *see also* Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distribs. & Northwest Nexus, Inc., 983 F. Supp. 1167, 1179 (N.D. Ill. 1997) (rejecting vicarious liability because the contract specified fixed fees). *But see* Playboy Enters. v. Webbworld, Inc., 968 F. Supp. 1171, 1177 (N.D. Tex. 1997) (finding a bulletin board service operator vicariously liable in spite of its flat fee arrangement because the presence of infringing content attracted users to the site).

161 *See* A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023–24 (9th Cir. 2001), *aff'g in part and rev'g in part* 114 F. Supp. 2d 896 (N.D. Cal. 2000).

162 A relevant example is the current doubt over the economic feasibility of providing free Internet access by ISPs. *See* Jason Anders, *Internet Firms Revise Free-Service Strategy*, WALL ST. J., Mar. 22, 2001, at B14.

163 17 U.S.C. § 512 (Supp. V 1999).

tion of ISP liability so far, in coping with ISP overdeterrence.[164] I will first examine the DMCA's effect on the costs of contracting between subscribers and ISPs over censorship practices adopted by ISPs. I will then analyze the extent to which the DMCA provides service providers with incentives to detect user misconduct.

Congress enacted Title II of the DMCA to limit ISP liability for copyright infringement by their subscribers.[165] The DMCA essentially creates a series of affirmative defenses, or "safe harbors," for service providers that might have been found liable for copyright violations under traditional principles of copyright law.[166] The requirements for enjoying these safe harbors depend on the type of service provided. The DMCA generally distinguishes among four types of services—transitory digital network communications, system caching, storage of information at the direction of users, and information location tools—and provides each type of service with different rules.[167]

1. *Incentive Divergence Under the DMCA*

As Part II argues, the severity of the ISP overdeterrence phenomenon depends on the cost of contracting between ISPs and their subscribers over screening and removal policies. Part III introduces the legal strategy of regulating the ISP-subscriber interface, which seeks to facilitate such contracting between the parties.[168] The DMCA does adopt several measures affecting the cost of contracting over monitoring policies between service providers and users. However, it seems that the DMCA did not go far enough in facilitating contracting between service providers and their subscribers.

To begin, the DMCA requires service providers to notify their users of their policy of terminating accounts of repeat infringers.[169] This requirement, by providing subscribers with information concerning termination policies, somewhat reduces their costs of transacting with service providers. However, the DMCA does not require service providers to notify their users of other aspects of their compliance

---

164 For an insightful, comprehensive analysis of the DMCA, see David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 680–82 (2000).

165 For a review of the legislative history of Title II of the DMCA, see Beams, *supra* note 51, at 831–41.

166 The DMCA defines "service provider" as a "provider of online services or network access, or the operator of facilities therefor." 17 U.S.C. § 512(k)(1). Courts have not yet determined the scope of Internet services covered by this definition.

167 *See id.* § 512(a)–(d).

168 *See* discussion *supra* Part III.B.

169 17 U.S.C. § 512(i)(1)(A).

policies, such as the technology that they employ to screen for copyright infringement.[170]

Moreover, the DMCA includes additional provisions that might *impede* contracting over removal policies by service providers. The most important measure is the immunity from liability granted to service providers that remove materials from the Internet.[171] This immunity not only further encourages service providers to disregard the cost associated with their screening policies and their removal decisions, but also potentially impedes any attempt to contract over monitoring policies between service providers and their users.[172] This potentially perverse effect of the immunity granted to service providers is somewhat alleviated by two other provisions of the DMCA. First, the DMCA imposes liability on copyright owners who provide service providers with false allegations that induce the ISP to remove legitimate materials from its networks.[173] This provision clearly aims at discouraging copyright owners from making false allegations to ISPs, and thereby at reducing the risk of ISP overdeterrence. In addition, in order to enjoy the immunity for the removal of materials, the ISP must notify the subscriber immediately and give it the opportunity to respond and dispute the removal decision.[174] By limiting the immunity to service providers that notify their users, the DMCA provides service providers with incentives to notify their subscribers of removal decisions.[175]

---

170 Indeed, as will be discussed below, the DMCA does not require service providers to monitor. Nevertheless, some monitoring will still be required for service providers that do not qualify for a safe harbor under the DMCA.

171 *See id.* § 512(g)(1) (baring service provider liability for claims "based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing").

172 *See* Yen, *supra* note 14, at 1888 (arguing that this immunity provision would induce ISPs to engage in excessive censorship).

173 17 U.S.C. § 512(f) (imposing liability on any person who makes a knowingly false claim of infringement that results in the removal or disabling of access to the relevant material). The deterrent effect produced by this section will not eliminate overdeterrence to the extent ISPs will be required to remove infringing materials even without a notice from copyright holders.

174 *See id.* § 512(g)(2). Under this provision, the ISP needs to take reasonable steps promptly to notify the subscriber that it has removed the material. *Id.* § 512(g)(2)(A). The subscriber is then granted the opportunity to dispute the decision by providing the service provider with a "counter notification." *Id.* § 512(g)(2)(B). Upon the receipt of such counter-notification, the service provider has to enable access to the material unless the copyright holder files an action seeking a court order. *Id.* § 512(g)(2)(C). For further analysis of these sections, see Jane C. Ginsburg, *Copyright Legislation for the "Digital Millennium"*, 23 COLUM.-VLA J.L. & ARTS 137, 162–63 (1999).

175 *Cf.* Communications Decency Act of 1996, 47 U.S.C. § 230(c)(2) (Supp. V 1999). This section provides that:

> No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to

These preconditions to ISP immunity, however, apply only to the providers of hosting services. Other service providers, such as the providers of Internet access, are not required to follow notification requirements to qualify for this immunity.[176] This particular result is very problematic. Subscribers of Internet access services are less likely than website operators to learn about their service providers' decision to block access to a particular site. Moreover, even when subscribers of access services learn about their ISP's decision to block access to a specific site, collective action problems will most likely impede their ability to dispute that decision. Therefore, subscribers of access services should enjoy greater protection than should subscribers of hosting services.[177] This protection could be achieved by granting users a right to sue their access providers in case they unjustifiably blocked Internet access, or by imposing mandatory disclosure requirements on access providers who seek to block access.[178] In any event, the DMCA fails to provide sufficient protection to subscribers of access services. This failure is very significant because it is very likely that the emergence of distributed peer-to-peer file exchange services in the aftermath of the *Napster* injunction would increase the pressure of content providers on access providers to prevent the access of their users to these file-sharing networks.[179]

> or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or any action taken to enable or make available to information content providers or others the technical means to restrict access to [said material].

Id. Unlike the DMCA, the Communications Decency Act does not impose notification requirements on ISPs.

176 The DMCA undoubtedly applies to access service providers. *See* Markiewicz, *supra* note 141, at 435–37 (stating that access service providers are included under § 512(a) of the DMCA).

177 As emphasized in the text, this argument applies only to a decision by a service provider to filter a particular site. Clearly, a subscriber would find out easily that her access provider has decided to terminate her account and prevent her from accessing the Internet.

178 One might argue that there is no need to grant subscribers greater protections because access providers will satisfy their condition for safe harbor much more easily than hosting-service providers. Thus, the risk of overdeterrence of access providers is less significant. Nevertheless, given the ambiguity of the DMCA, access providers are still exposed to a substantial risk of liability.

179 *See* John Borland, *Post Napster Policing Reopens ISP Wounds*, CNET NEWS.COM, Mar. 27, 2001 (reporting pressure of copyright holders on Internet access providers to police file-swapping networks), *at* http://news.cnet.com/news/0-1005-200-5263497.html. Recently, however, the music industry has re-adopted the strategy of directing its enforcement effort at companies offering users the ability to exchange files. *See* Gwendolyn Mariano, *Music Publishers File New Copyright Suit*, CNET NEWS.COM, Nov. 20, 2001 (reporting a recent lawsuit brought by the National Music Publishers' Association against three companies offering file-swapping services: MusicCity, Grokster, and Kazaa), *at* http://investor.cnet.com/investor/news/newsitem/0-9900-1028-7935995-0.html; John Borland, *Suit Hits Popular Post-Napster Network*, CNET NEWS.COM, Oct. 3, 2001 (reporting similar lawsuits,

2. *Monitoring Regulation*

A monitoring-regulation model of ISP liability is expected to specify the optimal level of policing that should be adopted by ISPs that wish to avoid liability.[180] The DMCA, however, explicitly declines to impose monitoring duties on service providers.[181] One might perceive this failure to impose monitoring duties as an expression of Congress's general position, applicable even outside the copyright context, that ISPs should not monitor user conduct. I find this interpretation to be flawed. The unwillingness to impose affirmative monitoring duties on service providers for copyright infringement is best viewed as expressing a position about the optimal level of ISP monitoring in the specific context of copyright, where copyright holders have superior ability to detect copyright infringement. Imposing strict liability on service providers will leave copyright owners with no incentives to assist in acquiring information about infringement by subscribers.[182] As copyright holders are often better positioned than the dispersed ISP industry to detect online infringement, it might be desirable to impose on them the burden of acquiring information about copyright infringement.[183] Under this logic, ISPs, although exempt from monitoring obligations concerning copyright, should be subjected to affirmative monitoring duties concerning unlawful conduct, such as online child pornography, with respect to which they are better positioned than the state, or the victims, to detect wrongdoing.

Indeed, while the DMCA does not impose affirmative monitoring duties on service providers, it provides elaborate regulations addressing copyright holders' role in providing service providers with information about infringement, especially with respect to the providers of hosting services. The DMCA limits the monetary liability of hosting-services providers that have no knowledge of infringement.[184] This

---

against the same defendants, filed by movie studios and record labels), *at* http://news.cnet.com/news/0-1005-200-7389552.html.

180 *See* discussion *supra* Part III.C.

181 *See* 17 U.S.C. § 512(m)(1) (Supp. V 1999) (cautioning against reading the section as imposing a duty on a service provider to monitor its service or affirmatively seek facts indicating infringing activity). Of course, if a service provider fails to meet the conditions for immunity under the DMCA, it might face monitoring duties under the traditional regime of copyright liability.

182 *See* SHAVELL, *supra* note 23, at 11 (emphasizing that imposing strict liability on the injurer provides victims with no incentive to exercise caution); *see also* A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023–24 (9th Cir. 2001) (emphasizing the role of the music industry in detecting infringement on the Napster system, and requiring record companies to provide notice of copyrighted music available for download on the system).

183 *But see* Ginsburg, *supra* note 174, at 162 (contending that this failure to provide ISPs with monitoring incentives under the DMCA leaves copyright holders with inadequate protection).

184 17 U.S.C. § 512(c)(1). The DMCA also requires that the ISP would derive no financial benefit from the infringing activity. *See id.* § 512(c)(1)(B).

immunity requires, however, that the ISP appoint an agent whom copyright owners can notify, and that this agent's contact information appear on the ISP's website.[185] The DMCA also elaborates on the precise notice that should be sent by copyright owners to ISPs.[186] Finally, ISPs are required to accommodate any standard technical measures taken by copyright owners to identify or protect their works.[187] Together, these regulations reflect the perception that, in the copyright context, copyright holders should bear the burden of detecting copyright infringement.

C. Auction Sites

Auction sites offer subscribers the opportunity to auction various items through their online systems. The subscriber posts the items she wishes to sell on the auction site. The operator of the site maintains the site and its auction software, notifies sellers and successful bidders when the bid is complete, and offers additional services to facilitate the transaction, such as online payments.[188] In return for these services, auction sites charge fees whose maguitude is proportional to the sale price of items auctioned through their system.[189]

The issue of auction-site liability arises when subscribers use the service to sell illegal items, such as bootlegged music or illegal drugs.[190] Recently, the desirable scope of auction-site liability for illegal items offered for sale by its subscribers has received public attention following a controversial decision by a French court requiring Yahoo! to block all French users from buying Nazi memorabilia on its auction site.[191] Recent public interest notwithstanding, the current rules that govern the liability of the providers of online auctioning

---

185 *Id.* § 512(c)(2).

186 *Id.* § 512(c)(3).

187 *Id.* § 512(i)(1)(B).

188 *See, e.g.*, eBay Inc., *Seller Guide, at* http://pages.ebay.com/help/sellerguide/index.html (last visited Jan. 19, 2002).

189 *See, e.g.*, eBay Inc., *Fees, at* http://pages.ebay.com/help/sellerguide/selling-fees.html (last visited Jan. 19, 2002).

190 *See* Kelley E. Moohr, *Going Once, Going Twice, Sold! Are Sales of Copyrighted Items Exposing Internet Auction Sites to Liability?*, 21 LOY. L.A. ENT. L. REV. 97, 98 (2000) (observing that "eBay has . . . become a hotbed for unauthorized sales of copyrighted works"); Mylene Mangalindan, *Alleged Drug Sale on eBay Raises Liability Issue*, WALL ST. J., May 30, 2000, at B18 (reporting a case in which high school students allegedly purchased drugs in an eBay auction).

191 See generally Carl S. Kaplan, *Ruling on Nazi Memorabilia Sparks Legal Debate*, N.Y. TIMES, Nov. 24, 2000, *at* http://www.nytimes.com/2000/11/24/technology/24CYBERLAW.html (last visited Jan. 19, 2002), for a history of the controversy. In the aftermath of this decision, Yahoo! announced a policy of screening hateful and violent materials out of its auctions, classified section, and shopping areas. Lisa Guernsey, *Yahoo to Try Harder to Rid Postings of Hateful Material*, N.Y. TIMES, Jan. 3, 2001, at C2.

services in the United States are yet to be clarified by courts.[192] This subpart argues that auction sites should be liable for illegal items auctioned through their systems under a standard of strict liability with reduced penalties.

Like many other providers of Internet services, auction sites do not capture the full value of the items they would be entrusted with policing under the liability regime I offer. Auction sites, however, currently charge their subscribers fees for each item posted for sale. Moreover, the size of these fees is determined according to the sale price of the item posted on the site. Auction sites will thus suffer an additional cost for any item that they decline to auction. The cost borne by the auction site will be proportional to the value of the item removed from the system. As explained above,[193] under these circumstances the ISP overdeterrence phenomenon could be mitigated, and perhaps even eliminated, by combining a regime of strict ISP liability with scaled-down penalties.

Moreover, because the cost of ex post negotiation between auction sites and their subscribers is relatively low, the incentives of auction sites will tend to aligu with those of their users. Sellers whose items have been rejected as unlawful will most likely learn very quickly about this rejection. The ability of subscribers to learn promptly of removal decisions substantially reduces the risk of excessive censorship. Furthermore, because a seller who believes that his item has been wrongfully rejected has an incentive to contact the auction site and dispute this decision, there is no collective action problem. Finally, switching costs, those associated with offering the item for sale on alternative sites, are negligible for subscribers of auction sites.

To be sure, as dictated by the economic theory of third-party liability, auction sites should be held liable only for sales that could be easily identified as illegal by existing monitoring technologies. Consider the difference between the sale of a photograph of Michael Jordan bearing his fake signature and the sale of a software labeled by the seller as "pirated." Determining the legal status of the Michael Jordan photograph requires the inspection of the photograph itself, which is transferred directly from the seller to the successful bidder. An auction site is thus unable to police items for misconduct of this type, and it would be undesirable to make it strictly liable for such

192 A recent decision by a California state court held that § 230 of the Communications Decency Act, 47 U.S.C. § 230, granted immunity to eBay for facilitating the auctioning of infringing sound recordings. *See* Stoner v. eBay, Inc., No. 305666, 2000 WL 1705637, at *3–*5 (Cal. Super. Ct. Nov. 1, 2000). Meanwhile, eBay, surrendering to pressure exerted by software makers and other intellectual property interests, has adopted a policy of monitoring its site for sales of infringing items. Simpson, *supra* note 75.

193 *See supra* Part III.A.

subscriber misconduct. The liability of auction sites should evidently be limited to the sale of items of the second type.[194]

CONCLUSION

The Internet's prompt, accurate, and inexpensive distribution of digital information encompasses a clear promise for human prosperity. However, the fascinating capabilities of the Internet also produce greater opportunities for unlawful conduct and challenge conventional strategies of law enforcement. The failure of the existing methods of law enforcement effectively to prevent online wrongdoing has sparked legal attempts to target the providers of Internet services and hold them liable for their subscribers' misconduct. Unfortunately, while policymakers and courts have been struggling in recent years to strike the appropriate balance between the need to prevent online misconduct and the risk of inhibiting the growth of the Internet, the issue of ISP liability has received little consistent theoretical treatment by legal scholarship.

In this Article, I attempted to fill this gap and provide the first step on the way to rectifying the balkanized analysis of ISP liability. ISPs are third parties harnessed by the legal system to police the conduct of primary wrongdoers, their subscribers. While ISPs possess the technical ability to prevent user misconduct, they do not capture the full value of the conduct they are entrusted with policing. Thus, subjecting ISPs to strict liability for the full social harm produced by subscriber misconduct will result in excessive monitoring and overzealous censorship. The Article has identified the role of contractual costs and market forces in aligning the incentives of ISPs with those of their subscribers, and the ensuing implications for designing an optimal ISP liability regime.

But for a brief discussion illustrating the illuminative power of the incentive-divergence thesis, the Article has been mostly devoted to developing a framework for evaluating optimal liability standards for ISPs. Designing an optimal ISP liability regime for a particular context requires a careful examination of the type of the service at stake and of the nature of the misconduct involved. The type of the service at stake determines the extent to which market forces could be relied upon to mitigate the severity of the divergent incentives. The nature of the misconduct determines the extent to which ISPs are positioned to distinguish between lawful and unlawful subscriber conduct. As the commercial use of the Internet is still evolving, it is very likely that

194 *See also Ebay's Liability Is Cleared in Suit*, N.Y. TIMES, Jan. 20, 2001, at C14 (reporting a San Diego court's dismissal of a class action suit against eBay brought on the grounds that the company had a responsibility to ensure the authenticity of the items sold through its website).

courts will need to rely on this framework and adapt it to pathbreaking Internet-related services and, unfortunately but inevitably, innovative Internet crimes.