INTERNET SERVICE PROVIDERS' VICARIOUS LIABILITY VERSUS REGULATION OF COPYRIGHT INFRINGEMENT IN CHINA

Ke Steven Wan†

TABLE OF CONTENTS

Abstract

The relative anonymity of individual subscribers forces copyright owners to increasingly seek to hold Internet Service Providers ("ISP") liable for the misconduct of their subscribers. ISP vicarious liability, however, also has limitations and disadvantages. There is no consensus about the scope of such liability, and ISPs are not in a good position to deter copyright infringement effectively in all contexts. Additionally, because ISP vicarious liability increases the price of Internet access, it may have an inevitable tradeoff

† Assistant Professor, City University of Hong Kong School of Law. S.J.D., LL.M., University of Pennsylvania Law School. I would like to thank Llewellyn Gibbons, Gideon Parchomovsky and two anonymous reviewers for their valuable comments on earlier drafts of this article. I would also like to thank the University of Illinois Journal of Law, Technology & Policy for its excellent editorial work. The study is supported by the Start-up Grant from the City University of Hong Kong.

between preventing copyright infringement and the market distortions it causes. Potential vicarious liability may drive out law-abiding subscribers as well as copyright infringers. In this situation, regulation of copyright infringement may be an appealing alternative. The purpose of the article is to provide academics and policymakers with a consistent framework for evaluating the relative desirability of ISP liability and regulation of copyright infringement. By taking China as an example, I discuss the four determinants of the framework in detail.

I. INTRODUCTION

The Internet has made reproduction and distribution of copyrighted materials easier than ever before, and has consequently made law enforcement more problematic. The relative anonymity of individual subscribers forces plaintiffs and law enforcers to increasingly seek to hold Internet Service Providers ("ISP") liable for the misconduct of their subscribers. In 1998, the Digital Millennium Copyright Act ("DMCA") incorporated a series of affirmative defenses, or "safe harbors," for ISPs that otherwise might have been found secondarily liable for their subscribers' acts of infringements.[1] *Religious Technology Center v. Netcom* is the first case to consider whether an ISP is liable for the infringing acts of its subscribers.[2] In this case, the court held the ISP was not liable because it received a flat monthly fee.[3] In *A&M Records v. Napster*, the court was the first to hold an ISP vicariously liable for copyright infringement.[4] Napster might have enjoyed § 512 immunity provided by the DMCA.[5] However, because Napster's revenue depended on

1. *See* 17 U.S.C. § 512 (2006). There are three terms to describe a service provider: Internet Service Provider (ISP), Online Service Provider (OSP) and Internet Access Provider (IAP). Section 512 of the DMCA has expanded the legal definition of Online Service Provider. A service provider is defined as either "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received," or "a provider of online services or network access, or the operator of facilities therefore." *Id.* § 512 (k). Under the DMCA, OSPs include both traditional ISPs and IAPs, which provide Internet access to subscribers. This broad definition allows a large number of web businesses to benefit from the DMCA. When I use "ISP" in this article, it broadly refers to "a business or organization that offers user access to the Internet and related services." In other words, OSPs and ISPs are used interchangeably for the purpose of this article. They provide services such as Internet transit, domain name registration and hosting, dial-up access, leased line access, and colocation. These ISPs not only offer Internet access, but also allow subscribers to communicate with each other and access the information on the Internet.

2. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1365 (N.D. Cal. 1995).

3. *Id.* at 1376.

4. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023–24 (9th Cir. 2001).

5. *See* 17 U.S.C. § 512(c) ("A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider—

(A)

(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which

"increase in userbase" and more copyrighted music generally attracted more users, the court held that Napster derived a financial benefit directly attributable to copyright infringement.[6] Napster was a vicarious infringer and was thus ineligible to avail itself of § 512 safe harbor provisions.[7]

ISP vicarious liability, however, also has limitations and disadvantages.[8] There is no consensus about the scope of such liability,[9] and ISPs are not in a good position to deter copyright infringement effectively in all contexts.[10] Additionally, because ISP vicarious liability increases the price of Internet access, it may have an inevitable tradeoff between preventing copyright infringement and the market distortions it causes.[11] Potential vicarious liability may drive out law-abiding subscribers as well as copyright infringers. In this situation, regulation of copyright infringement may be an appealing alternative.[12]

This article aims to add two contributions to the analysis of ISP liability and regulation of online copyright infringement in China. First, government regulation is more desirable than ISP liability in preventing online copyright infringement in China. In a previous article, the author generally compared the relative desirability of gatekeeper liability and regulation of wrongdoers based on four determinants.[13] Applying those four determinants to the context of online copyright infringement, this article concludes that regulation of copyright infringement is more desirable than ISP liability in China.

Second, I examine three concerns relating to regulation of copyright infringement in China, one of which is that a lack of anonymity may have a

---

the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.").

6. *A&M Records*, 239 F.3d at 1023.

7. *Id.* at 1025.

8. *See* John C. Coffee, Jr., *Gatekeeper Failure and Reform: The Challenge of Fashioning Relevant Reforms*, 84 B.U. L. REV. 301, 310 (2004) (discussing possible reasons for gatekeeper failure); Assaf Hamdani, *Gatekeeper Liability*, 77 S. CAL. L. REV. 53, 60 (2003) (arguing that gatekeeper liability may cause market distortions).

9. Coffee, *supra* note 7, at 308–09 (defining gatekeepers as those who have significant reputational capital and receive a far smaller benefit or payoff than the principal); Hamdani, *supra* note 7, at 63 (defining gatekeepers as those who "offer a service or sell a product that is necessary for clients wishing to enter a particular market or engage in certain activities"); Howell E. Jackson, *Reflections on Kaye, Scholer: Enlisting Lawyers to Improve the Regulation of Financial Institutions*, 66 S. CAL. L. REV. 1019, 1050–54 (1993) (defining gatekeepers as those who provide indispensable service, have ability to monitor wrongdoing, and cannot be easily replaced by wrongdoers); Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53, 53 (1986) (describing gatekeepers as "private parties who are able to disrupt misconduct by withholding their cooperation from wrongdoers").

10. The desirability of imposing liability on gatekeepers depends on whether they are in a good position to deter misconduct at acceptable costs. For example, accountants and lawyers may detect and deter corporate fraud in their relationship with the clients. Employers are well positioned to screen out illegal immigrants in their firms. ISPs can block access to illegal gambling sites at low costs. Peter Svensson, *Minnesota Asks ISPs to Block Gambling Sites*, ASSOCIATED PRESS, May 2, 2009, *available at* http://abcnews.go.com/Technology/story?id=7486035. With the content identification technology, ISPs may also be able to filter copyright infringement at reasonable costs. Expanding liability to those private parties can greatly reduce the social costs of enforcing the law.

11. Hamdani, *supra* note 7 (arguing that strict liability may distort the market for gatekeeper service).

12. *Id.* at 60–62.

13. *See generally* Ke Steven Wan, *Gatekeeper Liability Versus Regulation of Wrongdoers*, 34 OHIO N.U. L. REV. 483, 490–514 (2008).

chilling effect on speech. I analyze the costs and benefits of anonymity, arguing that anonymity in cyberspace should be limited because of the amplifying effect of the Internet. A danger of inappropriate disclosure of personal information, rather than a lack of anonymity, has a greater chilling effect on speech.[14] Even if the government avoids inappropriate disclosure of personal information, it can access private databases and cause harm to individuals.[15] Thus, government regulation of the Internet is likely to cause more harm than ISP monitoring. Because the Chinese government has been regulating Internet speech for a long time, however, an additional task of regulating copyright infringement should not have a more serious chilling effect on speech in China.

The article proceeds in three parts. Part II introduces the DMCA, European Union E-Commerce Directive and Chinese legislation and cases on ISP liability. Part III examines the necessity of ISP liability for copyright infringement. This Part discusses the weakness of direct liability and analyzes the tradeoff of ISP liability. Part IV compares ISP liability with regulation of copyright infringement in China based on four determinants. This Part analyzes three possible concerns about regulation of copyright infringement in China, including a chilling effect on speech, national favoritism, and rent-seeking.

II. DMCA, EU E-COMMERCE DIRECTIVE AND CHINESE LEGISLATION ON ISP LIABILITY

This Part introduces the legislation on ISP liability in three jurisdictions: United States, European Union, and China. This Part also points out the differences in legislation and analyzes the reasons for such differences where necessary.

Section 512 of the DMCA provides ISPs with "safe harbors."[16] ISPs are immunized from damages caused by: a) transitory digital network communications; b) system caching; c) information residing on systems or networks at the direction of users; and d) providing information location tools.[17] There are also several copyright enforcement mechanisms.[18] First, Section 512 introduces the notice and takedown procedure, which requires an ISP to expeditiously remove or block access to infringing materials upon notices from copyright owners.[19] Section 512 establishes strict requirements

14. *Cf.* Laura D. Ravine, *Footprints In Cyberspace: Using Transactional Data To Target Advertising*, 1998 UCLA J.L. & TECH. 4, ¶ 6 (1998) ("Americans are increasingly concerned about the lack of control they have over the collection and dissemination of their personal data.").

15. *See* E. Martin Estrada, *Criminalizing Silence: Hiibel And The Continuing Expansion Of The Terry Doctrine*, 49 ST. LOUIS U. L.J. 279, 305–06 (2005) (stating that American police officers have the ability to access "unparalleled amounts of personal information" using only the subject of a criminal investigation's name).

16. *See* 17 U.S.C. § 512 (2006) (outlining circumstances under which a service provider cannot be held vicariously liable for the actions of its subscribers).

17. *Id*. at §512(a)–(d).

18. Niva Elkin-Koren, *Making Technology Visible: Liability of Internet Service Providers for Peer-To-Peer Traffic*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 15, 29–30 (2005).

19. 17 U.S.C. § 512(c).

and procedures for proper notices.[20] Failure to comply substantially with statutory requirements will not be considered in determining the requisite level of knowledge by the ISP.[21] Second, Section 512 requires an ISP to disclose the identities of infringers upon subpoena requested by copyright owners.[22] Third, to be eligible for "safe harbors," an ISP must have "adopted and reasonably implemented, and inform[] subscribers . . . of, a policy that provides for the termination . . . of . . . repeat infringers,"[23] and "accommodates and does not interfere with standard technical measures."[24] There is, however, no affirmative duty for an ISP to monitor the network for copyright infringement.[25] An ISP's voluntary effort to monitor does not result in forfeiture of immunity within Section 512.[26]

Drafted by the European Commission, the E-Commerce Directive sets forth a limited liability regime for European ISPs.[27] Only three types of ISPs are afforded immunity: "mere conduit, caching, and hosting providers."[28] The Directive adopts a horizontal approach that provides immunity to "all types of illegal activities initiated by third parties, including copyright and trademark infringements, misleading publicity, acts of unfair competition, defamatory statements, pornography, etc,"[29] whereas the DMCA only applies to online copyright infringement.[30] Under the Directive, the immunity applies to both civil liability and criminal liability.[31] The Directive, however, only affords immunity to monetary damages rather than injunctions.[32] In other words, member states are permitted to grant injunctions according to their laws and regulations.[33] The Directive also provides a notice and takedown procedure similar to that in the DMCA.[34] The Directive emphasizes that there is no general obligation to monitor these three types of ISPs.[35] Consideration 48 of the Directive allows member states to establish a duty for their national ISPs to remove illegal materials.[36]

---

20. *Id*.
21. 17 U.S.C. at § 512(c)(3)(B)(i).
22. *Id.* at § 512(h)(1).
23. *Id.* at § 512(i)(1)(A).
24. 17 U.S.C. § 512(i)(1)(B).
25. 17 U.S.C. § 512(m).
26. MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.09[B](1) n.26 (2002); Jennifer Bretan, *Harboring Doubts about About the Efficacy of § 512 Immunity under Under the DMCA*, 18 BERKELEY TECH. L.J. 43, 51–52 (2003).
27. Patrick Van Eecke & Barbara Ooms, *ISP Liability & the E-Commerce Directive: A Growing Trend toward Toward Greater Responsibility for ISPs*, J. INTERNET L., Oct. 2007, at 3, 3.
28. *Id.* at 4.
29. *Id*.
30. 17 U.S.C. § 512(a) (2000). In the U.S., Section 230 also affords immunity to ISPs in various types of illegal activities initiated by third parties, including defamation and pornography.
31. Eecke & Ooms, *supra* note 26, at 4.
32. *Id*.
33. *Id*.
34. *Id.* at 5.
35. Council Directive 2000/31, art. 15, 2000 O.J. (L 178) 13 (EU).
36. Council Directive 2000/31, 2000 O.J. (L 178) 6 (EU) ("The Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.").

China has the largest population of Internet users in the world,[37] and the high rate of online copyright infringement in China has become a global problem. One commentator has noted that "[p]iracy went from being a small local enterprise to a major export industry[,] with Chinese-made pirated copies of US films, recordings, and computer programs showing up as far afield as Canada and Eastern Europe."[38] The Chinese government adopted legislation that provides ISPs with "safe harbors" from damages caused by the misconduct of their subscribers.[39] There are four major statutes or regulations concerning ISP liability in China: tort law,[40] Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Laws in Hearing Cases Involving Computer Networks Copyright Disputes (amended in 2006) ("Interpretations"),[41] the Measures on Administrative Protection of Internet Copyright ("Measures"),[42] and the Regulation on Protection of the Right to Network Dissemination of Information ("Regulation").[43] The Interpretations incorporate a "Notice and Take Down" procedure, which is similar to that of the DMCA.[44] Prior to the adoption of "safe harbors," under general tort

37. Guy Dixon, *China Becomes World's Biggest Internet Population*, V3 (Mar. 14, 2008), http://www.v3.co.uk/v3-uk/news/1962658/china-worlds-biggest-internet-population.

38. Greg Mastel, *China and the World Trade Organization: Moving Forward Without Sliding Backward*, 31 L. & POL'Y INT'L BUS. 981, 989 (2000).

39. Zuìgāo Rénmín Fǎyuàn Guānyú Shěnlǐ Shèjí Jìsuànjī Wǎngluò Zhùzuòquán Jiūfēn Ànjiàn Shìyòng Fǎlǜ Ruògān Wèntí De Jiěshì (最高人民法院关于审理涉及计算机网络著作权纠纷案件适用法律若干问题的解释) [Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Laws in Hearing Cases Involving Computer Networks Copyright Disputes] (promulgated by the Sup. People's Ct., Dec. 22, 2003, effective Dec. 22, 2003, amended Dec. 8, 2006), *translated in* China Internet Project, CHINA IT LAW, *available at* http://www.chinaitlaw.org/?p1=print&p2=060115231838 (last visited Sept. 26, 2010) [hereinafter *Chinese Interpretations*]. The Supreme Court's interpretation in China is similar to the agency interpretive rule in the U.S., which is legally binding.

40. Zhongua renmin zongghe guo qinquan zeren fa [Tort Liability Law of the People's Republic of China [Article 36]] 中华人民共和国侵权责任法(promulgated by Standing Comm. Nat'l People's Cong., Dec. 26, 2009), *translated in* 43 CHINESE LAW AND GOV'T, Sept.–Oct. 2010, at 82. The internet users and internet service providers shall assume tortious liability if they utilize the internet to infringe upon civil rights of others. *Id*. If an internet user commits a tort through utilizing internet services, the infringee shall be entitled to inform the internet service provider of taking necessary measures such as deletion, blocking and unlinking. *Id*. If the internet service provider fails to timely take necessary measures upon accepting notification, the internet service provider and the internet user shall assume joint liability for expanded damage. *Id*.

If an internet service provider knows that an internet user infringes the civil rights and interests of others through internet services thereof and fails to take necessary measures, the internet service provider and the internet user shall assume joint liability for the infringement. *Id*.

41. *Chinese Interpretations*, *supra* note 38.

42. Hù Lián Wǎng Zhù Zuò Quán Xíng Zhèng Bǎo Hù Bàn Fǎ (**互**联网著作权行政保护办**法**) [Measures for the Administrative Protection of Internet Copyright) (promulgated by the Nat'l Copyright Admin. of China and the Ministry of Info. Indus. on Apr. 30, 2005) (China), *translated in* China Internet Project, CHINA IT LAW, *available at* http://www.chinaitlaw.org/?p1=print&p2=051006180113 (last visited Sept. 26, 2010) [hereinafter *Chinese Measures*].

43. Xìnxī Wǎngluò Chuánbò Quán Bǎohù Tiáolì (信息网络传播权保护条例) [Regulation on Protection of the Right to Network Dissemination of Information] (promulgated by the St. Council, May 18, 2006, effective July 1, 2006), Arts. 22–23 (China), *Order No. 468 of the State Council, PRC*, CHINA IT LAW, *available at* http://www.chinaitlaw.org/ ?p1=regulations&p2=060717003346 (last visited Sept. 26, 2010) [hereinafter *Chinese Regulation*].

44. *See Chinese Interpretations*, *supra* note 38. *See also* 17 U.S.C. § 512(c). Section 512(c) establishes procedures for proper notification. First, an ISP must designate an agent to receive notifications of claimed infringement. *Id*. § 512(c)(2). The agent's contact information must be made readily available on the ISP's own site and through registration with the Copyright Office. *Id.* Second, to be an effective notice, a written communication to the designated agent of a service provider must contain specific identifying elements. *Id.*

principles, ISPs in China may have been jointly liable for the misconduct of subscribers, including copyright infringement and defamation.[45] The new legislation adds a series of affirmative defenses without changing the substantive standards of tort law with respect to ISPs.[46]

The Interpretations provide an ISP with immunity from damages if the ISP removes subscribers' unlawful content after receiving notice from copyright owners.[47] At the same time, the Interpretations impose liability on copyright owners who provide ISPs with false allegations of infringing content.[48] The provision intends to prevent copyright owners' false allegations and reduce the over-deterrence of ISPs.[49] Like the DMCA, the Chinese "safe harbor" provisions try to seek a balance among the interests of the copyright owner, the ISP, and the subscriber. There are certainly differences between the DMCA and the Chinese "safe harbors," but the general structure is the same.[50]

---

§ 512(c)(3)(A). The specific identifying elements must include identification of the infringing material, and information reasonably sufficient for the ISP to locate the infringing material, which is crucial in determining the scope of the subpoena power. *Id.* Failure to comply substantially with statutory requirements will not be considered in determining the requisite level of knowledge by the ISP. *Id.* § 512(c)(3)(B). An ISP is afforded immunity from damages if it expeditiously removes or blocks access to the infringing material upon notification. *Id.* § 512(d)(2). Furthermore, an ISP is generally not liable for any good faith removal, whether or not the material is actually infringing. *Id.* § 512(g)(1).

In order to prevent erroneous or fraudulent notifications, Section 512(g) provides subscribers with opportunities to respond to the removal of materials. *Id.* To qualify for safe harbors, an ISP is required to notify subscribers in § 512(c) takedown, but has no obligation to do so in § 512 (d) takedown. *Id.* § 512. The subscriber can respond to the removal by filing a counter notification, which includes identification of the material that has been removed or disabled, and a statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled through mistake or misidentification. *Id.* § 512(g)(3). If the counter notification complies with statutory requirements, the ISP must put the material back within 10-14 business days after receiving the counter notification, unless the copyright owner files an action seeking a court order against the subscriber first. *Id.* § 512(g)(2)(C). An ISP is immunized from liability for putting the material back, regardless of whether the material is actually infringing. *Id.* § 512(g)(4).

45. *See Chinese Interpretations*, *supra* note 38 (describing liability for the misconduct of subscribers).

46. *Id.* art. 46 ("If a network service provider participates in a copyright infringement with others via the Internet, or aided and abetted others to commit a copyright infringement via the Internet, the People's Court may investigate the contributory infringement liability of the provider with the other actors, or the actors, or the actors that committed the infringement on their own, in accordance with the stipulation of Article 130 of the General Principles of Civil Law.").

47. *Id.*

48. *Id.*

49. Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901, 951 (2001–02).

50. For example, there are the notice-and-takedown procedure and subpoena provisions in both the DMCA and the Interpretation. 17 U.S.C. § 512(c), (h) (2006); *Chinese interpretations*, *supra* note 38, art. 5–9. The Regulations provide four safe harbors for ISPs, similar to those in Section 512 of the DMCA: (1) transitory digital network communications, (2) system caching, (3) information storage, and (4) search or linkage service. § 512(a)–(d); *Chinese Regulation*, *supra* note 42. The conditions for those safe harbors in the Regulation, however, are a little different from those under Section 512. § 512(a)–(d); *Chinese Regulation*, *supra* note 42, art. 6–12. To qualify for information storage safe harbor, the Regulation requires ISPs to acquire no economic interests directly from the work. *Id.* To qualify for search or linkage service safe harbor, however, there is no such requirement. *Id.* Under Section 512, the conditions for the two safe harbors are essentially the same, both requiring ISP to receive no direct financial benefit. § 512(a)–(d), (i),(1), (m).

To prevent mistaken removal, the Measures provide that subscribers can file a counter notification, and an ISP may restore the content after receiving the counter notification. *Chinese Measures*, *supra* note 41, art. 7–10. The Regulations provide that an ISP "*shall* immediately resume the work, performance or audio and video recording being expurgated, or *may* resume the blocked link to the work, performance or audio and video recording", after receipt of counter notification. *Chinese Regulation*, *supra* note 42, art. 17. It seems that different restoration standards apply to information storage and search engine takedown. While restoring information storage takedown is mandatory after receipt of counter notification, it is up to the ISP to decide whether to resume the link to works in search engine takedown. *Chinese Measures*, *supra* note 41, art. 7–10;

Although the Interpretations deal with the contributory liability of ISPs, there are no specific statutes in China concerning an ISP's potential vicarious liability, and most judges in China are not familiar with vicarious liability.[51] Most Chinese courts held ISPs liable under contributory liability by interpreting an ISP's duty of care broadly.[52] One example is *Youdu v. Xunlei*, a seminal case to hold an ISP liable for providing deep linking in China.[53] Xunlei launched a dedicated video channel, enabling its users to search for movie resources on third-party websites. Additionally, it implemented framing and deep linking to movies for download.[54] The court held that "in view of the specific nature of Defendant's linking service, it has a higher duty of care to legality of the movies to which it linked for download than general search engines."[55] A commentator notes that courts seem to distinguish between two types of deep linking when interpreting ISPs' duty of care; while it is illegal to implement deep linking to audio or video files without copyright owners' consent, it is permissible to set up deep linking to text.[56] The court's decision is not without criticism, however. Another commentator argues that it is unnecessary to distinguish between the two kinds of deep linking when courts determine ISPs' duty of care.[57] Deep linking is no different from ordinary

Chinese Regulation, *supra* note 42, art. 17. Under Section 512, however, there is no such distinction between hosting service and search engine removal. § 512. In addition, while ISPs are required to record certain information under the Measures, there are no corresponding requirements in the DMCA. § 512. *But see Chinese Measures*, *supra* note 41, art. 6 ("Upon receipt of the Notice from the copyright holder, an Internet Information Service Provider shall record the content of the provided information, the time of its dissemination, Internet Protocol address or domain name accordingly. The Internet access service provider shall record the information of the Internet content provider such as the access time, user account, Internet Protocol address or domain name and the telephone number of the caller. The records as mentioned in the preceding paragraph shall be kept for 60 days and shall be furnished upon enquiry by the departments in charge of copyright administration.").

51. *See Chinese Interpretations*, *supra* note 38 (observing the lack of vicarious liability for ISPs in the Interpretations).

52. [Youdu v. Xunlei], (2007) 浦民三（知）初字第 69 号. *See also* [Go East Entertainment v. Alibaba], (2007）二中民初字第 02627 号; (2007）高民终字第 1191 号.

53. [Youdu v. Xunlei], (2007) 浦民三（知）初字第 69 号.

54. *Id. See also* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.01(A)(2) (Matthew Bender rev. ed. 2011) (arguing US court practice of holding deep linking illegal is wrong); Orit Fischman Afori, *Implied License: An Emerging New Standard In Copyright Law*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 275, 301–02 (2009) ("Under linking and framing, when a reader clicks on the link (which may be either highlighted text, an icon, or a picture), the user's web browser reads the software code, finds the location on the Internet that matches the address, and requests a copy of the web page. The computer hosting the linked web page sends the copy back to the user's browser. The browser on the user's computer reads the code of the copied web page and constructs the page according to the transmitted code, so that the page appears on the user's computer screen. Access to the content of the linked-to website is confirmed by the display of its Universal Resource Locator ("URL"), which replaces the URL of the previous website on the top portion of the user's browser. Deep linking refers to linking to an internal page of a website located at a lower level (or possibly several levels down) from the home page, thereby circumventing the home page and any other intervening pages. Framing differs from linking in that it allows a user to view the content of the linked site without leaving the site he or she is currently visiting, by calling up the content of the new webpage within the borders of the page being viewed. The technique enabling framing is similar to that of linking.").

55. [Youdu v. Xunlei], *supra* note 51.

56. Jiang Qingyun, 江清云，从德国司法判决比较超链接的著作权侵权界定，《德國研究》[*Copyright infringement caused by deep linking from the perspective of German cases*], [GERMAN STUDES] (2008/02).

57. Mao Zhimin, *毛之敏,設鏈行為之間接侵權的認定—兼評優度訴迅雷案一審判決*, *電子知識產權* [*Indirect liability of linking—Comments on* Youdu v. Xunlei], [ELECTRONICS INTELLECTUAL PROPERTY] (2008).

linking except that all the webpage converting is done backstage and is thus difficult to discern.[58] Xunlei did not reproduce or distribute copyrighted materials and should not be held directly liable.[59] Its contributory liability should also be limited by the safe harbor provisions.[60]

Another cause of confusion comes from the comparison between the *Yahoo China* case and the *Baidu* case.[61] Although both Yahoo China and Baidu offer essentially the same music search service, providing links to illegal music on third-party websites, Yahoo China lost whereas Baidu won.[62] Record companies sent two types of notices to Yahoo China: notices with URL addresses where suspected materials appeared and those without URL addresses.[63] Despite the lack of URL addresses, the court ruled that since record companies had provided the title of the song, the name of the singer, and the album in the notice, Yahoo China should have known of specific copyright infringement and should be held contributorily liable for its failure to remove infringing materials.[64] By contrast, Baidu was held not liable because the notices sent by record companies did not include URL addresses and were held to be insufficient to fulfill their obligation to notify Baidu [65] Commentators criticize the *Yahoo China* decision, arguing that the court inappropriately interpreted ISP's duty of care.[66] But Wang Qian distinguishes the *Yahoo China* case from *Fanya v. Baidu*,[67] noting that while providing merely the song title is insufficient to fulfill the obligation to notify, specifying the title of the song, the name of the singer, and the album, like in the *Yahoo China* case, is sufficient.[68] To what extent the notice triggers ISPs' duty of care remains a murky issue even today.

The lack of vicarious liability in Chinese law forces judges to interpret ISPs' duty of care broadly, resulting in inconsistent decisions and endless debate. If China adopts a vicarious liability regime, this may effect a dramatic change in Chinese copyright law, especially as applied in the context of the Internet. Copyright owners have a difficult time locating actual infringers in cyberspace, such that they are unable to sue the appropriate person in court.

---

58. *Id.*

59. [Youdu v. Xunlei], *supra* note 51.

60. See *Chinese Interpretations*, *supra* note 38, art. 4–5.

61. [Universal Music Ltd. v. Alibaba], (2007) 高民终字第 1190 号; [Universal Music Ltd. v. Baidu], (2005)一中民初字第 8474 号. *See also* Ting Low, *From Baidu to Worse*, 20(2) ENT. L.R. 64, 64–67 (2009); Xie Guanbin & Shi Xueqin, 谢冠斌，史学清，网络搜索服务商过错责任的合理界定—再评"雅虎案"与 "百度案"一审判决,《知识产权》[Determination of search engines' fault liability—Comments on "the Yahoo China case" and "the Baidu case"], [INTELLECTUAL PROPERTY], 2008/01(2008/01) ; Liu Xiaochun, 刘晓春，何為"明知或應知—評環球唱片訴阿里巴巴一審判決書, 《網絡法律評論》[What is "know and should have known"—Comments on Universal Music Ltd. v. Alibaba], [INTERNET LAW REVIEW], 171 (2010/01). *But see* Wang Qian, 王迁, 三論"信息定位服務提供者"間接侵權的認定—兼評"泛亞訴百度案"一審判決, 《知识产权》[Information Location Tool Providers' indirect infringement—Comments on Fanya v. Baidu], [INTELLECTUAL PROPERTY], (2009/02); Liu Jiarui, 刘家瑞, 论我国网络服务商的避风港规则——兼评"十一大公司诉雅虎案", 《知识产权》, [Internet Service Providers' safe harbors—comments on Eleven Companies v. Yahoo China], [INTELLECTUAL PROPERTY], (2009/02).

62. Low, *supra* note 60, at 64–67.

63. [Universal Music Ltd. v. Alibaba], *supra* note 60.

64. *Id.*

65. [Universal Music Ltd. v. Baidu], *supra* note 60.

66. Xie Guanbin & Shi Xueqin, *supra* note 60; Liu Xiaochun, *supra* note 60.

67. [Fanya v. Baidu], (2007）高民初字第 1201 号.

68. Wang Qian, *supra* note 60.

As ISPs may have deep pockets and are easy to find, copyright owners are highly likely to add ISPs as third-party defendants in almost every copyright infringement case. Unable to risk monetary damages in addition to a court injunction, ISPs will eventually have to take measures against subscribers' copyright infringement.

In sum, the legislation in all three jurisdictions affords immunity to certain types of ISPs and introduces the notice and takedown procedure. There are, however, differences in the scope of immunity and specific provisions. In the next part, I will discuss the rationale to hold ISPs liable for subscribers' copyright infringement.

III. WHY ISP LIABILITY FOR COPYRIGHT INFRINGEMENT?

Deterrence theory requires lawmakers to hold wrongdoers liable for infringement.[69] Direct liability may fail to act as a deterrence when wrongdoing is expensive for the victim to detect or for the government to prosecute. The conditions of the Internet make it very difficult to penalize individual wrongdoers. The relative anonymity of Internet subscribers makes the detection of wrongdoers very costly.[70] Even if caught, infringers often turn out to be judgment-proof individuals, who lack sufficient assets to pay damages.[71] Some people might argue that criminal liability could be a substitute. However, it may not be cost-effective to impose criminal liability, especially imprisonment, on infringers.[72] The cost of imprisonment includes: the prosecutorial cost, the wages of guards, buildings, food, etc. .[73] Unlike the

69. *See* Hamdani, *supra* note 48, at 910 ("Deterrence theory seeks to impose on wrongdoers the social cost of their wrongdoing.").

70. *Id*.

71. *Id*. at 910–11. *See also* 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) (noting that college students, who may not have the resources to pay large judgments, were sued by the government in many of the most notorious Internet criminal prosecutions); 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 copyright infringers are individuals who "do not have enough assets to make legal action worthwhile").

72. *See* Aaron Rappaport, *Litigation over Prison Medical Services*, 7 HASTINGS RACE & POVERTY L.J. 261, 282 (2010) ("[I]n many cases we have overstated the benefits of prison, while ignoring its enormous fiscal and human costs."). *See also* Robin Andrews, Note, *Copyright Infringement and the Internet: An Economic Analysis of Crime*, 11 B.U. J. SCI. & TECH. L. 256, 262 –63 (2005) (discussing the economic costs of crime and law enforcement); Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 179–80 (1968) (discussing resource allocation and how much punishment should be used to enforce different kinds of legislation); V.S. Khanna, *Corporate Criminal Liability: What Purpose Does it Serve?*, 109 HARV. L. REV. 1477, 1532–33 (1996). It is also unfair to impose harsher punishment on innocent violation of copyright law than medical malpractice. *See* Geraldine Szott Moohr, *The Crime of Copyright Infringement: An Inquiry Based on Morality, Harm, and Criminal Theory*, 83 B.U. L. REV. 731, 747–52 (2003) (discussing the rationale for treating conduct as criminal); LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 199–202 (Penguin Press 2004). There are other equitable concerns as well. A legal system where only a small fraction of wrongdoers are penalized and suffer extremely harsh penalties is unjust. *See* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 234 n.36 (2006); Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395, 408 (2003) (discussing different forms of indirect liability). *See also* Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 596–599 (2001) (discussing intermediary liability in defamation cases).

73. Becker, *supra* note 71, at 180; Sara Sun Beale, *Solutions: Is Corporate Criminal Liability Unique?*,

case of civil damages, nobody gets what the prisoner loses. Besides, extreme criminal penalties may distort legitimate use of the Internet and have a chilling effect on technology development.[74] Hence, it is sometimes impossible to impose direct liability on wrongdoers. Expanding liability to third parties is a solution to deal with the under-deterrence of Internet subscribers.[75] In the context of online copyright infringement, manufacturers of computers, developers of Internet browsers, and makers of modems are all candidates for the imposition of third-party liability.[76] Lawmakers should only expand liability, however, to those parties who are in a good position to deter misconduct cost-effectively.[77]

One commentator defines the cheapest cost avoider as the party who can avoid the accident at the lowest overall cost.[78] Guido Calabresi and Jon Hirschoff define the cheapest cost avoider as the party who "is in the best position to make the cost-benefit analysis between accident costs and accident avoidance costs and to act on that decision once it is made."[79] The party who is in the best position to make the cost-benefit analysis is not necessarily the one that acts upon it.[80] The cheapest cost avoider test has been traditionally applied to product manufacturers.[81] Judges only need to decide the cheapest cost avoider between the injurer and the victim.[82] In online copyright infringement, however, courts need to determine the cheapest cost avoider among the copyright owner, the direct infringer, and the ISP.

If copyright owners can determine the cheapest cost avoider, should courts let them "bribe" the ISP—the cheapest cost avoider—to prevent infringement? Professor Ronald Coase notes that "[w]henever accident costs exceed the cheapest cost avoider's prevention costs," the party bearing accident costs will bargain with the cheapest cost avoider to prevent the accident.[83] No matter the initial allocation of liability, market forces will

---

44 AM. CRIM. L. REV. 1503, 1512 (2007).

74. Richard A. Posner, *An Economic Theory of the Criminal Law*, 85 COLUM. L. REV. 1193, 1206 (1985) ("If there is a risk either of accidental violation of the criminal law or of legal error, an expected penalty will induce innocent people to forgo socially desirable activities at the borderline of criminal activity.").

75. *See* Reinier H. Kraakman, *Corporate Liability Strategies and the Costs of Legal Controls*, 93 YALE L.J. 857, 888–96 (1984) (noting that third-party liability is necessary to address the failure of direct liability).

76. *See* Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1864 (2000) (noting that nearly all information technology providers could be held liable).

77. *See* Kraakman, *supra* note 8, at 100–01 (proposing a four-part test for the desirability of gatekeeper liability). *See also* Hamdani, *supra* note 48, at 910–11 (discussing the expansion from subscriber only liability to ISP liability via third-party liability).

78. Stephen G. Gilles, *Negligence, Strict Liability, and the Cheapest Cost-Avoider*, 78 VA. L. REV. 1291, 1307–08 (1992).

79. Guido Calabresi & Jon T. Hirschoff, *Toward a Test for Strict Liability in Torts*, 81 YALE L. J. 1055, 1060 (1970). *See also* Richard W. Wright, *The Principles of Product Liability*, 26 REVIEW LITIG. 1067, 1099 (2007) (analyzing why product manufacturers are the cheapest cost avoider).

80. Calabresi & Hirschoff, *supra* note 78, at 1060 n.19.

81. *See* GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 136 (1970) (applying the cheapest cost avoider test to car manufacturers). *See also* Thomas C. Galligan, Jr., *Strict Liability in Action: The Truncated Learned Hand Formula*, 52 LA. L. REV. 323, 344 (1991); David G. Owen, *Rethinking the Policies of Strict Product Liability*, 33 VAND. L. REV. 681, 711–12 (1980) (emphasizing a willingness to assume manufacturers are to blame for product accidents).

82. Calabresi & Hirschoff, *supra* note 78, at 1060–61.

83. Richard D. Cunningham, *Apportionment Between Partmakers and Assemblers in Strict Liability*, 49 U. CHI. L. REV. 544, 549–50 (1982). *See also*, Guido Calabresi, *Transaction Costs, Resource Allocation and*

ensure that the cheapest cost avoider bears the prevention costs in the absence of transaction costs.[84] Legal rules do not affect the efficient outcome in a perfect market without transaction costs because voluntary transactions of rational individuals will make the best use of resources.[85] Government intervention is considered economically undesirable in a perfect market.[86] In the case of copyright infringement, if copyright owners have a right to enjoin the third-party, they can sell the right. If the third-party has the right to sell products or services with impunity, it can sell the right. The party who values the right to infringe more will buy it from the other if necessary.[87] Transaction costs, however, may disrupt the negotiation and transaction between parties.[88]

The market may incur two types of transaction costs. First, the search for the cheapest cost avoider may incur transaction costs;[89] second, the cheapest cost avoider may charge a premium in exchange for bearing the prevention costs.[90] Depending on parties' bargaining power, the premium can be as high as their differences in prevention costs.[91] Due to ISPs' market power, they are highly likely to charge a significant premium. The failure to reach an enforcement agreement after years of negotiations between copyright owners and ISPs suggests that the premiums charged by ISPs exceed the amount that copyright owners are willing to pay. Because the transaction costs may be higher than the administrative costs of judicial allocation of accident costs,[92] it is more desirable for lawmakers to impose liability on the ISP.

The economic literature regarding primary wrongdoing assumes that it is desirable to make wrongdoers "internalize the social cost of their wrongdoing."[93] The reason is that, even if they cannot prevent wrongdoing,

---

Liability Rules—A Comment, 11 J.L. & ECON. 67, 67 (1968) (analyzing the Coase Theorem and arguing that it is as equally valid in the long term as it is in the short term); Harold Demsetz, *The Exchange and Enforcement of Property Rights*, 7 J.L. & ECON. 11 (1964) (discussing the Coase Theorem and the role of governments and markets in economic life); Harold Demsetz, *When Does the Rule of Liability Matter*?, 1 J. LEGAL STUD. 13 (1972) (discussing the Coase Theorem and analyzing how legal liabilities will affect the allocation of resources).

84. *See generally* R. H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 42–44 (1960) (articulating what is currently known as the Coase Theorem).

85. Marianne M. Jennings & Stephen Happel, *The Post-Enron Era for Stakeholder Theory: A New Look at Corporate Governance and the Coase Theorem*, 54 MERCER L. REV. 873, 910–11 (2003); Mark MacCarthy, *What Payment Intermediaries Are Doing About Online Liability and Why It Matters*, 25 BERKELEY TECH. L.J. 1037, 1047–1051 (2010). *See* ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS, 82–96 (2d ed. 1997); Coase, *supra* note 83, at 5–6; 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, 264–65 (2001).

86. Yen, *supra* note 84, at 258–59.

87. *Id.* at 264–65.

88. *Id.*

89. *See* CALABRESI, *supra* note 80, at 136–38 (explaining the affect that transaction costs have on the search for the cheapest cost avoider).

90. *See generally* Richard D. Cunningham, *Apportionment Between Partmakers and Assemblers in Strict Liability*, 49 U. CHI. L. REV. 544, 549–51 (1982); Harold Demsetz, *Wealth Distribution and the Ownership of Rights*, 1 J. LEGAL STUD. 223, 224–27 (1972) (explaining that insurance companies charge premiums in exchange for taking on risk).

91. *Id.* at 550 ("Depending on the parties' relative bargaining positions, th[e] premium can range anywhere from just above zero to just below the difference between their prevention costs. . . .").

92. *Id.* (explaining that in "many situations" the costs of judicial intervention are less than the costs associated with "private attempts to find the cheapest cost avoider").

93. Hamdani, *supra* note 48, at 60 n.24.

they can reduce their activity level.[94] For third parties, however, the scale of their activity "should not be adjusted to the social cost of wrongdoing."[95] The goal of third-party liability is to deter wrongdoing rather than scale down the activity level.[96] Commentators argue that deterrence, rather than fairness, should be the justification for vicarious liability.[97] A commentator supports indirect liability:

> [I]ndirect liability need not be conceived merely as a second-best solution to a discrete set of problems with direct liability. When some easily identifiable third-party is better positioned to monitor and control the behavior of the primary wrongdoer than a court or other government regulator, indirect liability will be more efficient than even perfectly functioning direct liability.[98]

Indirect liability is desirable when the third-party can detect and deter misconduct at low costs.[99] Commentators list examples of precautions an ISP can take. An ISP can detect subscribers' suspicious patterns of Internet use, such as "a continuous stream of communications from a home user or the repeated appearance of identical computer code attached to a large number of outgoing email messages."[100] An ISP can also keep a record of subscribers' activities for a period of time so that infringers can be discovered.[101] In addition, an ISP can alert other ISPs or customers about suspicious changes in traffic patterns so that they can locate the source of the threat or avoid the harm.[102] Because ISPs can control the content on their networks and potentially deter misconduct at acceptable costs, my article will assume that ISP liability is desirable.

In addition, ISPs and subscribers might be able to structure a contractual, cost-spreading mechanism to induce ISPs to behave in an optimal manner. ISPs interact with subscribers. They charge for Internet services, so if they have to pay for violations of subscribers, they can raise their prices accordingly. Because of the huge customer base, however, ISPs do not need to increase the price significantly. The *Polygram* court treated risk allocation as the justification for vicarious liability:

---

94. *Id*.

95. *Id*. *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, 573 (1988) ("By measuring those incremental costs with reference to the social costs that would otherwise arise if the resources used by the enterprise were unemployed, a resulting competitive equilibrium will tend to generate an efficient allocation of resources among alternative enterprises and alternative (nonenterprise) uses for the resources (such as leisure).").

96. Hamdani, *supra* note 48, at 912.

97. Gary T. Schwartz, *The Hidden and Fundamental Issue of Employer Vicarious Liability*, 69 S. CAL. L. REV. 1739, 1754, 1763–64 (1996); Ke Steven Wan, *Monopolistic Gatekeepers' Vicarious Liability For Copyright Infringement*, 23 REGENT U. L. REV. 65, 87–92 (2010) (exploring the rationales for vicarious liability such as deterrence and corrective justice). There are equity counterarguments, however. Some argue that ISPs should not be held vicariously liable merely because they are in a good position to prevent online copyright infringement. Alfred C. Yen, *Third Party Copyright Liability after* Grokster, 91 MINN. L. REV. 184, 213 (2006).

98. Daryl J. Levinson, *Aimster and Optimal Targeting*, 120 HARV. L. REV. 1148, 1154 (2007).

99. Lichtman & Posner, *supra* note 71, at 236–37.

100. *Id*. at 237.

101. *Id.* at 237–38.

102. *Id*.

> The law of vicarious liability treats the expected losses as simply another cost of doing business. The enterprise and the person profiting from it are better able than either the innocent injured plaintiff or the person whose act caused the loss to distribute the costs and to shift them to others who have profited from the enterprise. In addition, placing responsibility for the loss on the enterprise has the added benefit of creating a greater incentive for the enterprise to police its operations carefully to avoid unnecessary losses.[103]

There are two generally accepted types of cases involving vicarious liability: dance hall proprietors and landlords.[104] Numerous court decisions excuse landlords from liability[105] while dance hall proprietors are held vicariously liable for copyright infringement committed by performers.[106] The "dance hall cases" refers to dance halls which hire a performer to play music without obtaining a license.[107] Although the performer actually infringes the copyright, the dance hall operator could control the performances on its premises.[108] In addition, the dance hall operator receives admission fees from patrons, thus profiting directly from the infringing performance.[109] In contrast, a landlord exercises no control over tenants' premises and is not in a good position to do so.[110] The landlord receives a flat monthly rental rather than deriving direct financial benefit from infringement.[111] On one hand, an ISP resembles a dance hall proprietor because it has a strong ability to control activity on the network. On the other, an ISP is similar to a landlord because it usually receives a fixed service fee. The decisive prong of vicarious liability, as will be discussed later, is the right and ability to control, rather than "direct" financial benefit.[112] Although an ISP does not derive a direct financial benefit from infringement, infringing content often acts as a draw for subscribers.[113]

---

103. Polygram Int'l Publ'g, Inc. v. Nevada/TIG, Inc., 855 F. Supp. 1314, 1325 (D. Mass. 1994); Yen, *supra* note 96, at 219.

104. Yen, *supra* note 75, at 1844.

105. *See e.g.*, Deutsch v. Arnold, 98 F.2d 686, 688 (2d Cir. 1938) ("Something more than the mere relation of landlord and tenant must exist to give rise to a cause of action by the plaintiffs against these defendants . . . .").

106. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 436–37 n.18 (1984); Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262–63 (9th Cir. 1996); Shapiro, Bernstein & Co., Inc. v. H.L. Green Co., Inc., 316 F.2d 304, 307–08 (2d Cir. 1963); *Polygram*, 855 F. Supp. at 1324–25; Yen, *supra* note 75, at 1844–45. *See also* Banff Ltd. v. Limited, Inc., 869 F. Supp. 1103, 1108–09 (S.D.N.Y. 1994) (discussing vicarious liability logic similar to that in the "dance hall cases").

107. Yen, *supra* note 75, at 1844.

108. *Fonovisa*, 76 F.3d at 262.

109. *Id.*

110. *See* Artists Music Inc. v. Reed Publ'g (USA) Inc., No. 93 Civ. 3428, 1994 WL 191643, at *5 (S.D.N.Y. 1994) (explaining that landlords lack the ability to supervise tenants' use of leased premises). *See also* Yen, *supra* note 75, at 1844–45 (explaining that landlords exercise less control than tenants do over the leased property).

111. *See Shapiro*, 316 F.2d at 307 (noting that when a landlord charges a fixed rent is evidence that the landlord is not gaining any financial benefits from the infringement); Deutsch v. Arnold, 98 F.2d 686, 688 (2d Cir. 1938) (explaining that the landlord's connection to the acts of infringement must include more than the basic landlord-tenant relationship); *Artists Music*, 1994 WL 191643, at *6 (explaining that a landlord must be shown to have benefitted financially from the infringement); Vernon Music Corp. v. First Dev. Corp., No. 83-0645-MA, 1984 WL 8146, at *1 (D. Mass 1984) (holding that summary judgment is should be granted in favor of the landlord-defendant because it did not benefit financially from the plaintiff's activities).

112. Wan, *supra* note 12, at 75.

113. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023–24 (9th Cir. 2001) (explaining that

Thus, an ISP resembles a dance hall proprietor in light of this distinction.

There is a general consensus that ISPs should be compelled to facilitate prevention of copyright infringement.[114] There is controversy, however, over identifying the scope and standard of ISP liability for subscriber misconduct.[115] Acknowledging their unique position in the area of the Internet, ISPs do not want to become "deep pockets," who are likely to be added as third-party defendants in every online copyright infringement lawsuit. ISPs have argued that their liability for copyright infringement should be construed narrowly so that more entrepreneurs can enter the Internet industry and speed up its development.[116] Copyright owners, however, argue that ISPs should be held vicariously liable for all online copyright infringement on their networks because they are in a good position to deter infringement at low costs.[117] It is still unclear what the appropriate scope of ISP liability is for their subscribers' copyright infringement. In addition, ISP liability does not work well in all contexts. Assaf Hamdani discusses the market distortion effects of ISP liability[118] and indicates that government regulation may be an appealing alternative to deter wrongdoing.[119] He also suggests that policymakers weigh the costs of gatekeeper liability against the costs of regulation.[120]

To summarize, ISP liability is justified because of its ability to prevent copyright infringement on its network at low costs. There are, however, costs associated with ISP liability such as the market distortion effects. Government regulation may be a more appealing alternative to prevent online copyright infringement than ISP liability. In the next part, I will compare ISP liability with regulation of copyright infringement in China.

IV. ISP LIABILITY V. REGULATION OF COPYRIGHT INFRINGEMENT IN CHINA

This Part examines the relative desirability of ISP liability and regulation of copyright infringement in China, based on the four determinants in the context of gatekeeper liability: the difference in the information regarding illicit activities, the ability to compensate for harm done, a gatekeeper's ability to deter misconduct either through law or by architecture, and the costs incurred by private parties and by the public.[121]

Napster "benefits from the continuing availability of infringing files on its system").

114. Hamdani, *supra* note 48, at 911(explaining that ISP liability is justified because "Internet Service Providers [can] prevent subscriber misconduct cheaply").

115. BRUCE A. LEHMAN, INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 114–16 (1995).

116. *Id.* at 116; Mark E. Harrington, *On-Line Copyright Infringement Liability for Internet Service Providers: Context, Cases & Recently Enacted Legislation*, 1999 B.C. INTELL. PROP. & TECH. F. 60499, at ¶ 1 (June 4, 1999), http://www.bc.edu/bc_org/avp/law/st_org/iptf/articles/content/1999060401.html.

117. Yen, *supra* note 75, at 1835–36.

118. *See supra* text accompanying notes 9–10.

119. Hamdani, *supra* note 7, at 106–08 (explaining that ISP liability is a type of gatekeeper liability).

120. *Id*. at 107.

121. Wan, *supra* note 12, at 493–514; Steven Shavell, *Liability for Harm Versus Regulation of Safety*, 13 J. LEGAL STUD. 357 (1984).

A. ISP Liability v. Regulation: Examination of the Four Determinants in China

The first determinant is the difference in the information regarding illicit activities between private parties and a regulatory authority.[122] The difference is in relation to "the benefits of activities, the costs of reducing risks, or the probability or severity of the risks."[123] Steven Shavell notes that "private parties should generally enjoy inherent advantage in knowledge."[124] They participate in the activities and should naturally be in a better position to estimate the benefits and risks.[125] The government, by contrast, must continuously inspect private parties' behavior to collect comparable information, which is arduous and practically impossible.[126] Private parties do not possess superior knowledge of risk in all circumstances, however. The government enjoys an information advantage about risk where "risk will not be an obvious by-product of engaging in risky activities but rather will require effort to develop or special expertise to evaluate."[127] The government may commit social resources to the task during regular administration such as pollution prevention, while private parties may lack the incentive to obtain such information.[128] Shavell notes:

> A party who generates information will be unable to capture its full value if others can learn of the information without paying for it. For parties to undertake individually to acquire information might result in wasteful, duplicative expenditures, and a cooperative venture by parties might be stymied by the usual problems of inducing all to lend their support.[129]

The free rider problem dilutes private parties' incentive to investigate copyright infringement on the Internet because an infringing website may contain thousands of songs by hundreds of artists. Moreover, even if the government obtains the necessary information, it is difficult to inform copyright owners of the infringement because they are hard to identify and too numerous in cyberspace. Some might argue that copyright collective societies, such as the American Society of Composers, Authors, and Publishers ("ASCAP"), can solve the problem. Individual copyright owners, however, may disagree on the extent of protection and costs that should be spent on the detecting technology. The complex Internet and sophisticated wrongdoers also make it difficult for copyright owners to keep pace with the technological development. If detecting costs are sufficiently high, copyright owners will weigh detecting costs against losses resulting from copyright infringement. When detecting costs are much higher than the infringement losses, it may be desirable for the government to commit social resources to the task of

122. Shavell, *supra* note 120, at 359.
123. *Id.*
124. *Id.* at 360.
125. *Id.*
126. *Id.*
127. *Id.*
128. *Id.*
129. *Id.* (footnote omitted).

detection. In the context of online copyright infringement, the risk may not be obvious to copyright owners and may require expertise to evaluate. Thus, the government may have an information advantage relative to private parties in cyberspace.

The Musical Copyright Society of China ("MCSC") is the only officially recognized, non-profit social organization for the collective administration of music copyright in China.[130] It was established in 1992 and was initiated by the Chinese Musicians' Association and the National Copyright Administration of China.[131] The quasi-government background makes collective management societies a monopoly and impedes their development.[132] The Regulations on Copyright Collective Management provide that collective management societies shall be non-profit organizations.[133] During the past eighteen years, the MCSC has experienced difficulties with lack of funds and trained people, weak trade unions, users' reluctance to cooperate, and vastness of the territory it has to detect.[134] In addition, it lacked administrative supervision and was incomplete in system.[135] The fact that there were only about three thousand members with the MCSC after fifteen years of development proves its failure.[136] To facilitate the

130. *General Information*, MUSICAL COPYRIGHT SOC'Y OF CHINA, http://www.mcsc.com.cn/Introduction.php?partid=28 (last visited Sept. 22, 2011) [hereinafter MUSICAL COPYRIGHT].

131. *Id*.

132. *See* Regulations on Copyright Collective Administration (promulgated by the State Council of China, Mar. 1, 2005, effective Mar. 1, 2005), *translated* by CHINA PATENT AGENT (H.K.) LTD., http://www.cpahkltd.com/EN/info.aspx?n=20100315165402343027. (Article 6: "With the exception of copyright collective management organization established according to these Regulations, no organization or individual shall engage in activities of copyright collective management."). *Id.* art. 9 (Article 9: "Anyone applying for establishing a copyright collective management organization shall submit the materials proving the satisfaction of the conditions as stipulated in Article 7 of these Regulations to the administrative department in charge of copyright under the State Council. The administrative department in charge of copyright under the State Council shall make a decision on approval or disapproval within 60 days as of receipt of the materials. Approved, to issue the permit of copyright collective management; disapproved, to explain the reasons."). *Id.* art. 12 (Article 12: "The copyright collective management organization shall get approval of the administrative department in charge of copyright under the State Council when establishing branches, and shall go through the registration procedures with the civil administration department under the State Council according to administrative regulations concerning social association registration administration. The organization that has been registered according to law shall report the copy of certificate of registration of its branch to the administrative department in charge of copyright under the State Council for the record, and the administrative department in charge of copyright under the State Council shall announce it to the public."). *See also* Lu Haijun, 卢海君，论我国著作权集体管理组织的法律地位，《政治与法律》, [*The Legal Status of Collective Management Societies in China*], [POLITICS AND LAW], (2007/02).

133. *See* [Copyright Law of the People's Republic of China] (promulgated by Standing Comm. Nat'l People's Cong., Feb. 26, 2010, effective Jun. 1, 1991) (amended in 2010) (Article 8: "Organizations of collective management over copyright shall be non-profit organizations, and their establishment modes, rights and obligations, collection and allocation of copyright licensing fees, and supervision and management of these organizations shall be separately prescribed by the State Council."). *See also Regulations on Copyright Collective Administration*, WORLD INTELLECTUAL PROP. ORG., http://www.wipo.int/wipolex/en/text.jsp?file_id=181505 (last visited Sept. 22, 2011) (English version of Chinese full text regulation) (Article 42: "If a copyright collective administration organization is engaged in activities for profit purposes, it shall be banned, and its illegal income shall be confiscated according to law by the administrative department for industry and commerce. Where a crime is constituted, criminal liability shall be investigated according to law.").

134. MUSICAL COPYRIGHT, *supra* note 129.

135. Zhang Yaoming, *The Basic System of the Protection of Copyright*, 1 CHINA COPYRIGHT 11 (2005); Yuan Zeqing, *A New Impetus for Chinese Copyright Protection: the Regulations on Collective Administration of Copyright*, 28 EUR. INTELL. PROP. REV. 241, 241–42 (2006).

136. Haijun, *supra* note 131, at 71.

MCSC's development, a commentator suggests allowing the establishment of competing societies and eliminating the non-profit requirement in the law.[137] Although collective management societies in China may be strengthened in the future, even strong rights organizations like in the United States or European Union still fail.[138]

The Regulations on Copyright Collective Management entered into force in 2005 and were the first legislation for regulating copyright collective management societies in China.[139] However, no groups of copyright owners or users participated in the drafting process. The government dominated the process, with limited participation of social organizations and legal experts.[140] The ignorance of market forces may lead to an unfair rate of royalties and other problems. In addition, the quasi-government background of collective management societies and the resulting administrative intervention may reduce their impact on the Chinese copyright market. Although copyright collective management societies will undoubtedly play a crucial role in copyright protection in the long run, the government seems to have an information advantage relative to copyright owners in China at present, especially with its control over the backbone provider in China.[141]

The second determinant is an ISP's ability to compensate for harm done.[142] If losses exceed ISPs' assets, ISP liability may not be able to provide them with sufficient incentive to prevent wrongdoing.[143] ISPs go bankrupt, employees lose jobs, and shareholders lose investments. Assets would not affect the effectiveness of regulation, however, because the government will impose ex-ante regulation before copyright infringement occurs.[144] If an individual violates the ex-ante regulation, the government can imprison the wrongdoers or shut down the company. Because large ISPs generally have "deep pockets," they usually have sufficient assets to pay damages. Their assets are more vulnerable to seizures or liens than those of other online copyright infringers. The loss of assets would provide ISPs with sufficient incentive to prevent subscribers' copyright infringement. The determinant of inability to pay for harm done weighs in favor of ISP liability.

ISP liability insurance can also affect ISPs' ability to pay for harm done. Insurance is the art of calculating risk. If the information upon which such calculation should be based is unavailable, insurance may not exist on the market. Because it is the ISP's users who commit copyright infringement, the insurer may have difficulty in assessing the risk of ISP liability by monitoring

137. *Id.*

138. *See, e.g.*, Richard Hayes Phillips, *How One Independent Musician Defeated BMI*, WOODPECKER RECORDS (2003), http://www.woodpecker.com/writing/essays/phillips.html. *See also* Harvey Reid, *ASCAP & BMI—Protectors of Artists or Shadowy Thieves?*, WOODPECKER RECORDS, http://www.woodpecker.com/writing/essays/royalty-politics.html (last updated 2005) (noting many of the problems with ASCAP and BMI).

139. WORLD INTELLECTUAL PROP. ORG., *supra* note 132.

140. Zeqing, *supra* note 134, at 242–43.

141. Alex Wyatt, *The Global Economy and the On-Line World: Consequences of WTO Accession on the Regulation of the Internet in China*, 3 MELB. J. INT'L L. 436, 449 (2002).

142. Shavell, *supra* note 120, at 360.

143. *Id.* at 361.

144. *Id.* at 362.

an ISP's activities.[145] If copyright infringement occurs, ISPs and infringing users will be jointly liable under ISP liability.[146] Strict liability is generally more desirable than negligence or knowledge-based liability for ISPs.[147] The insurance market may collapse when strict liability is combined with joint and several liability.[148] However, because an ISP's precautions, such as the software to filter infringing materials, become more reliable in detecting copyright infringement, insurers may be better able to calculate the risk and provide ISP liability insurance.[149]

ISP insurance or IP insurance is rare even in the United States or European Union.[150] There are largely two types of IP insurance: IP defense insurance and IP abatement insurance.[151] While the former subsidizes litigation and defends the company against charges of IP infringement, the latter provides funds and services to commit the right owner to enforce its IP rights.[152] If ISP liability insurance is available, will ISPs purchase it? Unlike individuals, ISPs are generally sophisticated in spreading risk to subscribers. They interact with subscribers, so if they have to pay for subscribers' copyright infringement, they can raise their service price accordingly. In addition, the insurance premium increases an ISP's cost.[153] One empirical study shows, however, that most companies choose to purchase insurance.[154] Mayers and

145. *See* Kenneth S. Abraham, *Environmental Liability and the Limits of Insurance*, 88 COLUM. L. REV. 942, 955–56 (1988) (noting that uncertainty may undermine liability insurance market); *see also* STEVEN SHAVELL, ECONOMIC ANALYSIS OF ACCIDENT LAW 198 (Harvard Univ. Press 1987) (discussing that parties may have no insurance against certain types of risk).

146. *See Chinese Interpretations*, *supra* note 38.

147. Hamdani, *supra* note 7, at 59 (discussing the two advantages of strict liability).

148. Benjamin J. Richardson, *Mandating Environmental Liability Insurance*, 12 DUKE ENVTL. L. & POL'Y F. 293, 301–02 (2002) (discussing the "uncertainty surrounding the risks sought to be insured").

149. For an example of ISP insurance, see *ISP Insurance*, UNITED INSURANCE, INC., http://www.ispinsurance.com (last visited Sept. 22, 2011).

150. *See* Ian McClure, *Intellectual Property Insurance: Transforming the Economic Model for IP Litigation*, THE FEDERAL LAWYER, July 2010, at 18; *IP Abatement Insurance*, INTELL. PROP. INS. SERVS. CORP., http://www.ipisc.com/products/insurance-policies/abatement (last visited Aug. 30, 2011). Such insurance serves to help a rights holder pursue a claim. For a formal explanation, see Gerard Llobet & Javier Suarez, *Patent Litigation and the Role of Enforcement Insurance* (July 2008) (unpublished manuscript) (available at http:// www.cemfi.es/~llobet/PLpaper.pdf).

Although Errors & Omission (E&O) insurance is available to cover possible claims of copyright infringement, it primarily deals with filmmakers' direct liability, not ISPs' secondary liability. "Film-makers seeking E & O insurance do not deal directly with the insurer, but instead fill out an application with a broker. The application itself begins with the presumption that any copyrighted material within a documentary has been cleared with formal permission from the owner. The form asks if copyrighted materials are included within the film. If so, it then asks if permission to use it has been obtained from the owner. If permission has been denied, the film-maker must explain the refusal. In addition, the film-maker must provide a full clearance history of any copyrighted material included in the film, again explaining any failure to secure permissions. Finally, the applicant is asked if she has been party to an infringement claims, whether brought to fruition in proceedings, pending, or threatened; this demand extends to claims the film-maker may reasonably believe to potentially exist, within the last five years." Thomas Plotkin & Tarae Howell, *"Fair Is Foul and Foul Is Fair:" Have Insurers Loosened the Chokepoint of Copyright and Permitted Fair Use's Breathing Space in Documentary Films?*, 15 CONN. INS. L.J. 407, 456–57 (2009).

151. *See* McClure, *supra* note 149, at 18.

152. *Id*.

153. *See* SEAN J. GRIFFITH, *Uncovering a Gatekeeper: Why the SEC Should Mandate Disclosure of Details Concerning Directors' and Officers' Liability Insurance Policies*, 154 U. PA. L. REV. 1147, 1168–70 (2006) (noting that "it always costs more to buy insurance for a risk than to bear it oneself.").

154. *See* David Mayers & Clifford W. Smith, Jr., *On the Corporate Demand for Insurance: Evidence from the Reinsurance Market*, 63 J. BUS. 19, 19 (1990) (focusing on the corporate demand for insurance and

Smith explain the reasons:

> [F]or corporations with diffuse ownership risk aversion by the owners apparently provides no incentive for the purchase of insurance . . . . We argue that the corporate demand derives from the ability of insurance contracts to (1) allocate risk to those of the firm's claimholders who have a comparative advantage in risk bearing, (2) lower expected transactions costs of bankruptcy, (3) provide real-service efficiencies in claims administration, (4) monitor the compliance of contractual provisions, (5) bond the firm's real investment decisions, (6) lower the corporation's expected tax liability, and (7) reduce regulatory constraints on firms.[155]

China's insurance market is still in its infancy. A study demonstrates that Chinese companies' decisions to purchase insurance are "positively related to leverage and physical assets intensity, but negatively related to State ownership [and] tax rate."[156] As the Chinese market is a developing and risky one, lenders may require collateralized assets to be insured to mitigate potential losses.[157] "[T]he volume of property insurance purchased . . . is positively related to managerial ownership, foreign ownership and growth options . . . ."[158] As managerial share ownership increases in China, managers have greater incentives to purchase corporate insurance to reduce risks to job security and ill-diversified personal wealth.[159] The presence of State ownership could decrease the incentive to purchase corporate insurance, while the existence of high levels of foreign ownership seems to promote the procurement of corporate insurance.[160] In addition, companies with greater growth opportunities tend to be less risk-averse because their managers are usually given more discretion over investment decisions, which may be less transparent to outsiders such as creditors.[161] Thus, companies with high growth potential have a greater incentive to purchase insurance than those with low growth prospects.[162] In a developing market like China, many ISPs are regarded as having great growth potential and are therefore more likely to purchase corporate insurance to reduce risk.[163] In sum, the "deep pockets" of ISPs, in addition to possible insurance, make ISP liability more desirable than regulation.

The third determinant, according to Shavell, is "the chance that parties would not face the threat of suit for harm done."[164] Deterrence is diluted by the unlikely chance that direct infringers face the threat of suit for harm done

---

using reinsurance data to discuss corporate demand for insurance).

155. David Mayers & Clifford W. Smith, Jr., *On the Corporate Demand for Insurance*, 55 J. BUS. 281, 293 (1982) (discussing the reasons that corporations purchase insurance policies).

156. Hong Zou & Mike B. Adams, *The Corporate Purchase of Property Insurance: Chinese Evidence*, 15 J. FIN. INTERMEDIATION 165, 167 (2006).

157. *Id.* at 169.

158. *Id.* at 167.

159. *Id.* at 172–73 (noting one of two competing hypotheses "concerning the influence of managerial ownership on the corporate purchase of insurance reported in the financial literature").

160. *Id.* at 193.

161. *Id.* at 171.

162. *Id*.

163. *Id.*

164. Shavell, *supra* note 120, at 363.

under the ISP liability regime.[165] On one hand, many of the harms done by copyright infringement are sufficiently dispersed so that individual copyright owners lack incentive to bring suit.[166] On the other, even if copyright owners have sufficient motivation to bring lawsuits, they would prefer to sue ISPs rather than direct infringers because of the ease of locating ISPs and their sufficient assets.[167] Although it is possible for ISPs to detect IP addresses of the infringing computers, it is hard to trace the copyright infringement to particular persons.[168] Considering the high costs, ISPs are more likely to improve precautions on their networks rather than pursue anonymous wrongdoers.

The third determinant in the context of gatekeeper liability should be whether a gatekeeper can deter misconduct either through law or by architecture.[169] Architecture refers to a physical feature or to code in cyberspace in a human-built environment.[170] For example, in the real world, speed bumps act as an architectural constraint on speeding.[171] Architecture is "automated, immediate, and plastic."[172] It is self-enforcing and curtails the discretion afforded by law.[173] Unless people can circumvent the architecture, they are unlikely to commit infringement.[174] Architecture, then, may be a more cost-effective means of policing and enforcing than the law.[175]

Even if wrongdoers do not face the threat of infringement suit, ISP liability may still be desirable if the ISP can prevent copyright infringement by improving its architecture. Changes to ISP software architecture or code, such as the content identification technology, are likely to help ISPs deter copyright infringement without targeting wrongdoers.[176] Google has introduced a content identification tool for its video-sharing site Youtube.[177] Copyright owners have to first upload their movies or television clips in a Google database.[178] These movies or television programs are then splintered and compared with any uploaded video to check for copyright infringement.[179] The new technology does not prevent subscribers from uploading disputed videos.[180] It only helps copyright owners to identify their works on Youtube, and choose

165. *Id*.
166. *Id*.
167. Wan, *supra* note 12, at 506.
168. *Id*. at 507.
169. *Id*. at 506–08.
170. *Id*. at 508.
171. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 92 (1999).
172. James Grimmelmann, Note, *Regulation by Software*, 114 YALE L.J. 1719, 1729 (2005) (describing the three characteristics of software).
173. *Id*. at 1729–30.
174. *See id*. at 1730.
175. *Id*. at 1729.
176. *China to Release Content Identification Standards*, MARBRIDGE DAILY (Aug. 20, 2008), http://www.marbridgeconsulting.com/marbridgedaily/archive/article/18959/china_to_release_content_identification_standards?sk=b66495a953d63baeed1d4eb511bf956a&p=1&high=on.
177. Associated Press, *For YouTube, A System to Halt Copyright-Infringing Videos*, N.Y. TIMES, Jul. 28, 2007, at C6; Ellen Lee, *YouTube Introduces New Copyright Filter*, S.F. CHRON., Oct. 16, 2007, at B1; Thomas Claburn, *Google's YouTube Debuts Copyright Enforcement System*, INFORMATIONWEEK (Oct. 16, 2007, 3:50 PM), http://www.informationweek.com/news/202403363.
178. Claburn, *supra* note 176.
179. *Id*.
180. *Id*.

their strategy against the disputed videos: whether to block, promote, or even license the videos.[181] The Chinese Ministry of Culture has announced that "China will promulgate a national standard for identification codes to be used in online content such as music, video and text."[182] Pomoho.com and 56.com, the leading video sharing websites in China, announced commercial deployment of VideoDNA™ content identification and management system with Vobile, the leading provider of content identification technology.[183]

Although the content identification technology could assist ISPs in preventing online copyright infringement without pursing wrongdoers, it may have the drawback of defeating fair use.[184] The filter cannot distinguish outright copyright infringement from the legitimate inclusion of "copyrighted materials for parody, criticism and educational purposes."[185] Fingerprinting technology may be able to flag copyrighted material, but it cannot make judgment whether or not it is fair use.[186] In addition, IsoHunt, a BitTorrent search engine, resisted the permanent injunction imposed by the District Court of California and appealed to the Ninth Circuit: IsoHunt argued that a filter based on a list of keywords provided by the movie industry is a futile solution that would impede freedom of speech and introduce censorship to the United States.[187] Although it is unclear whether the permanent injunction on the BitTorrent search engine will stay in place, site-wide filtering by general search engines like Google would reignite fierce debate.[188] Thus, it remains to be seen whether an ISP is capable of accurately deterring copyright infringement by using architecture. Currently, regulation of copyright infringement seems to be superior to ISP liability in China under this determinant.

The fourth determinant is the costs incurred by private parties and by the public in using ISP liability and regulation.[189] The costs of ISP liability include the costs of litigation and the court system, as well as the expenses of an ISP in changing its architecture or monitoring users, etc.[190] Similarly, the

181. *Id.*

182. *China to Release Content Identification Standards*, *supra* note 175.

183. *See* Press Release, 56.com, 56.com Announces Commercial Deployment with Leading Provider of Video Content Identification Vobile (Mar. 23, 2009), *available at* http://www.56.com/press_room_en.html.

184. Greg Jansen, Note, *Whose Burden is it Anyway? Addressing the Needs of Content Owners in DMCA Safe Harbors*, 62 FED. COMM. L.J. 153, 175–178 (2010) (addressing the shortcomings of current video fingerprinting technology use); Eric Bangeman, *Consortium's User–Generated Content Principles Extend Far Beyond Fair Use*, ARS TECHNICA, http://arstechnica.com/tech-policy/news/2007/10/consortiums-user-generated-content-principles-extend-far-beyond-fair-use.ars (last visited Sept. 22, 2011).

185. Bangeman, *supra* note 183.

186. Jansen, *supra* note 183, at 176; Bangeman, *supra* note 183.

187. Ernesto, *IsoHunt Tells Court that MPAA's Filter is Needless Censorship*, TORRENTFREAK, (June 27, 2010), http://torrentfreak.com/isohunt-tells-court-that-mpaas-filter-is-needless-censorship-100627/.

188. Meng Ding, Perfect 10 v. Amazon.com*: A Step Toward Copyright's Tort Law Roots*, 23 BERKELEY TECH. L.J. 373, 397 (2008) ("Google should not be required to implement intensely complicated tools to counter access to infringing material because its general-purpose search engine serves a very wide audience, and the difficulty of blocking access to infringing material is high. Grokster, on the other hand, should be subject to a more stringent requirement of implementing filtering mechanisms to filter out infringing material because unlike Google, Grokster was exclusively engaged in music posting."); Jane C. Ginsburg, *Separating the* Sony *Sheep from the* Grokster *Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, 50 ARIZ. L. REV. 577, 587–88 (2008).

189. Shavell, *supra* note 120, at 363.

190. *Id.* at 363–64.

costs of regulation include "the public expense of maintaining the regulatory establishment and the private costs of compliance."[191] ISP liability seems to have an inherent advantage in terms of cost since most of the administrative costs are incurred only if harm occurs.[192] As this will happen infrequently, administrative costs should be low.[193] Unlike ISP liability, administrative costs of regulation are incurred regardless of whether harm occurs.[194] However, several factors may offset the disadvantage of regulation. On one hand, safety devices, such as fire extinguishers or lifeboats, make enforcement less costly.[195] On the other, probabilistic methods of enforcement are often used to reduce the costs.[196]

In addition, government regulation may be more desirable than ISP liability for two reasons. First, monitoring by the government is more cost-effective than monitoring by various ISPs because there are economies of scale in monitoring. A commentator proposes the centralized monitoring by an international organization because "such an organization could pool resources, achieve economies of scale, and thereby provide for greater efficiency."[197] Similarly, the centralized monitoring by the Chinese government is more cost-effective than monitoring by numerous ISPs in China.[198] Second, subscribers need to access the Internet through a backbone provider controlled by the government and are beyond legal control because of the relative anonymity of the Internet and their limited assets. The government is well-positioned to deter copyright infringement because it can control the content by redesigning distribution channels and making changes to its network.[199] The cost of network design changes is an empirical question. The fact that cyberspace is built on software, rather than brick and mortar, should make it cost-effective to modify the network design.

Administrative costs of regulation in China may be relatively low because of several reasons. First, under the Measures on the Regulation of Public Computer Networks and the Internet ("Network Regulation Measures"),[200] there is only one Internet gateway in China, which is operated by ChinaNet, a

191. *Id.* at 364.
192. *Id*.
193. *Id*.
194. *Id*.
195. *Id*. at 370.
196. *Id*.
197. Paul Przybylski, Note, *A Common Tool for Individual Solutions: Why Countries Should Establish an International Organization to Regulate Internet Content*, 9 VAND. J. ENT. & TECH. L. 927, 951 (2007).
198. *See id*. (noting the efficiency of a centralized system).
199. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 198–200 n.62 (1997) (noting that manufacturers and sellers, the cheapest cost avoider, can make changes to avoid damages); H. Brian Holland, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, 56 U. KAN. L. REV. 369, 392–93 (2008); Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 390–91 (2005). *See also* Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 240 (2005) (arguing that intermediaries are likely to be the cheapest cost avoiders in the online context because of "(1) an increase in the likelihood that it will be easy to identify specific intermediaries for large classes of transactions, (2) a reduction in information costs, which makes it easier for the intermediaries to monitor the conduct of end users, and (3) increased anonymity, which makes remedies against end users generally less effective").
200. *PRC Measures on the Regulation of Public Computer Networks and Internet*, C114 (Sept. 6, 2009),http://www.cn-c114.net/575/a287863.html (English version of Chinese full text regulation).

company under the control of the Ministry of Information Industry ("MII").[201] With such an Internet structure, the MII is able to monitor all information transmitted via the Internet in China,[202] block access to certain websites by placing a filter on the Internet gateway,[203] and even completely shut down the Internet in China by deactivating the Internet gateway.[204] It is obvious that the single-gateway structure of the Internet in China is a powerful tool to detect and deter online copyright infringement. By contrast, in most Western countries, there are multiple Internet gateways, many of which are owned by private companies.[205] The multiple-gateway structure of the Internet makes it more costly to deter misconduct.

Second, the Chinese government has already established a sophisticated system to filter the Internet speech.[206] China has spent six-hundred million yuan (U.S. $ 70 million) on efforts to regulate the Internet.[207] Rumor says that over thirty-five thousand "Internet police" are dedicated to enforcing China's Internet regulations.[208] The Chinese Communist Party ("CCP") regulates the Internet through "physical restrictions, regulations that dictate permissible use and ownership and operation of ISPs."[209] There are two levels of censorship of Internet speech. First, the Chinese government controls what its citizens can see by filtering out information flowing through the Internet gateway, which

201. Richard Cullen & Pinky D.W. Choy, *The Internet in China*, 13 COLUM. J. ASIAN L. 99, 105 (1999); Wyatt, *supra* note 140, at 449.

202. Wyatt, *supra* note 140, at 449.

203. *Id*.

204. *Id*.

205. *Id*.

206. Anne S.Y. Cheung, *The Business Of Governance: China's Legislation On Content Regulation In Cyberspace*, 38 N.Y.U. J. INT'L L. & POL. 1, 2 (2006). *See* Richard Cullen & D.W. Choy, *China's Media: The Impact of the Internet*, 6 SAN DIEGO INT'L L.J. 323, 328–29 (2005) (describing China's use of the Internet to improve government administration and disseminate propaganda). *But see* Aaron D. McGeary, *China's Great Balancing Act: Maximizing The Internet's Benefits While Limiting Its Detriments*, 35 INT'L LAW 219 (2001) (concluding that China's attempts to regulate the Internet have proven unsuccessful); *China's Internet Censorship*, CBSNEWS.com (Jan. 11, 2010), http://www.cbsnews.com/stories/2002/12/03/tech/main531567.shtml; Alfred Hermida, *Behind China's Internet Red Firewall*, BBC NEWS ONLINE (Sept. 3, 2002), http://news.bbc.co.uk/2/hi/ technology/2234154.stm; Ethan Gutmann, *US/China: Up Against the Firewall*, 119 RED HERRING, Nov. 2002, at 48, *available at* http://www.corpwatch.org/article.php?id=4854; David Lee, *Multinationals Making a Mint from China's Great Firewall*, S. CHINA MORNING POST, Oct. 2, 2002, at 16; Howard W. French, *Chinese Censors and Web Users Match Wits*, N.Y. TIMES, Mar. 4, 2005, at A10.

207. *See* Jeffrey Hays, *Great Firewall. Censorship, Blocked Sites and Government Control of the Internet in China*, FACTS & DETAILS (last updated Mar. 2011), http://factsanddetails.com/china.php?itemid=232; Martin Fackler, *China Looks Abroad for Latest Technology to Police Internet*, AP, (Nov. 8, 2000) http://abcnews.go.com/Technology/story?id=119309&page=1.; Aaron D. McGeary, *China's Great Balancing Act: Maximizing The Internet's Benefits While Limiting Its Detriments*, 35 INT'L LAWYER 219, 230 (2001).

208. *The Internet in China: A Tool for Freedom or Suppression?:Hearing Before the Subcomm. on Afr., Global Human Rights and Int'l Operations and the Subcomm. on Asia and the Pacific of the Comm. on Int'l Relations*, 109th Cong. 157 (2006) (testimony of Harry Wu, Publisher, China Information Center); Marc D. Nawyn, *Code Red: Responding to the Moral Hazards Facing U.S. Information Technology Companies in China*, 2007 COLUM. BUS. L. REV. 505, 519–20 (2007). *See* generally Rebecca MacKinnon, *Digital Silk Road Conference: The Internet in China*, RCONVERSTATION (Jun. 1, 2005), http://rconversation.blogs.com/rconversation/2005/06/digital_silk_ro.html (detailing the technology used by the Chinese government to police the Internet).

209. Clara Liang, Note, *Red Light, Green Light: Has China Achieved its Goals Through the 2000 Internet Regulations?*, 34 VAND. J. TRANSNAT'L L. 1417, 1428–29 (2001) (describing how physical restrictions refer to China's effort to build an intranet and construct a firewall).

connects China with the outside world.[210] Second, because the Internet gateway does not prevent access to content already inside a domestic network, the Chinese government relies on the cooperation of regional ISPs to filter information that does not have to pass through the Internet gateway.[211] The most prevalent forms of Internet filtering include Internet Protocol ("IP") address blocking and content filtering. IP address blocking refers to preventing users from accessing specific IP addresses.[212] This would prohibit users from accessing any content on the blocked site whether or not the content is objectionable.[213] Content filtering, however, is more finely grained and prohibits users from accessing any site containing certain keywords, phrases, or even images.[214] The filtering technology can even allow the government to detect the forbidden words or other "content" within the IP packets travelling between users' computers and targeted sites.[215] Since the Chinese government spares no effort to regulate the Internet speech, an additional task of deterring copyright infringement should not dramatically increase the administrative costs.

Third, a probabilistic method of enforcement can be used to lower the administrative costs. Wrongdoers will be subject to random inspection by the regulatory authority, in contrast to an almost no threat of infringement suit under the ISP liability regime.

In addition, obstacles to administrative enforcement in the physical world are no longer problems in cyberspace. Similar to judicial protection, administrative protection suffers from local protectionism, low damages, and inappropriate sales of infringing equipment at public auctions in China.[216] Commentators suggest centralizing copyright enforcement.[217] The local support and resources needed to protect copyright in such a large country, however, may prevent the central government from accomplishing the task.[218] Unlike piracy in the physical world, online copyright infringement can be deterred without local support. The characteristics of the Internet and

210. Eric Harwit & Duncan Clark, *Shaping the Internet in China: Evolution of Political Control over Network Infrastructure and Content*, 41 ASIAN SURV. 377, 378 (2001); Nawyn, *supra* note 207, at 511–13.

211. Nawyn, *supra* note 207, at 514–15; "*Race to the Bottom": Corporate Complicity in Chinese Internet Censorship*, HUMAN RIGHTS WATCH (Aug. 10, 2006), http://www.hrw.org/reports/2006/china0806/china0806web.pdf.

212. Nawyn, *supra* note 207, at 510; *Internet Filtering in China in 2004–2005: A Country Study*, OPENNET INITIATIVE (Apr. 15, 2005), http://opennet.net/sites/opennet.net/files/ONI_China_Country_Study.pdf.

213. Nawyn, *supra* note 207, at 510; OPENNET INITIATIVE, *supra* note 211.

214. Nawyn, *supra* note 207, at 510–11; OPENNET INITIATIVE, *supra* note 211.

215. Nawyn, *supra* note 207, at 7 (stating that the Chinese government uses Cisco 12000 series routers, which "have packet filtering capacity, allowing the routers to filter bi-directionally at the packet level . . .").

216. Maria C.H. Lin, *China After the WTO: What You Need to Know Now* (817 PLI Com. L. & Prac. Handbook Series Order No. A0-0095, 2001). *See* Andrew Evans, Note, *Taming the Counterfeit Dragon: The WTO, TRIPS and Chinese Amendments to Intellectual Property Laws*, 31 GA. J. INT'L & COMP. L. 587, 591 (2002–03); *Snags Hit IPR Fight*, S. CHINA MORNING POST, Apr. 13, 1995, at 11; *The Discreet Charm of Provincial Asia*, THE ECONOMIST, Apr. 27, 1996, at 85. *See also* Jeffrey W. Berkman, *Intellectual Property Rights in the P.R.C.: Impediments to Protection and the Need for the Rule of Law*, 15 UCLA PAC. BASIN L.J. 1, 20 (1996–97).

217. *See* Peter K. Yu, *From Pirates to Partners: Protecting Intellectual Property in China in the Twenty-First Century*, 50 AM. U. L. REV. 131, 151–59 (2001). *See also* CHIH-YU SHIH, COLLECTIVE DEMOCRACY: POLITICAL AND LEGAL REFORM IN CHINA 255, 300 (1999).

218. *See* CHIH-YU SHIH, *supra* note 216, at 300; Yu, *supra* note 216, at 159.

information technology make it possible to centralize the copyright enforcement in cyberspace.

By contrast, several factors may result in high administrative costs of the ISP liability regime in China. First, the enforcement of court decisions is still a big problem.[219] While Beijing courts enforced 90% of the judgments made by Beijing Courts from 2003 to 2006,[220] the nationwide enforcement rate is much lower, varying from 40% to 60%, according to chief of the Supreme People's Court's Judgment Enforcement Division.[221] Copyright owners may not be able to obtain damages from defendants even if they win the cases, although injunctions might be available.

Second, the difficulty of collecting evidence makes judicial protection unappealing. Most copyright owners find that the best way to obtain evidence of piracy is through a raid and seizure action.[222] Such a procedure, however, is normally pursued through administrative authorities of copyright.[223] In addition, it is difficult for copyright owners to transfer such evidence to courts for civil litigation because there are no guidelines on the transfer of such evidence.[224] Collecting evidence is no longer a problem in cyberspace, however, because copyright owners will often save a copy of the infringing work on their computers. Also, the infringing work is often recoverable even if deleted.

Third, local protectionism, judicial corruption, public distrust of judges, and a lack of intellectual property training among judicial personnel remain major problems in the judicial enforcement of copyright laws.[225] Overall evaluation indicates that the administrative cost of regulation may appear lower per party than that under the ISP liability regime in China, although the cost of the ISP liability regime may be reduced in the future.[226]

Evaluating the above four determinants, three of the four favor regulation—information advantage, deterrence through law or by architecture, and administrative costs—and only one favors the ISP liability regime—inability to pay for harm done. Overall balance should indicate the relative desirability of substantial regulation of online copyright infringement in China.

---

219. Brent T. Yonehara, *Enter the Dragon: China's WTO Accession, Film Piracy and Prospects for the Enforcement of Copyright Laws*, 9 UCLA ENT. L. REV. 389, 407–08 (2002). *See also* Berkman, *supra* note 215, at 24–26; Robert Slate, *Judicial Copyright Enforcement Iin China: Shaping World Opinion on TRIPS Compliance*, 31 N.C. J. INT'L L. & COM. REG. 665, 684–87 (2006).

220. *Courts Struggle with Judicial Enforcement*, THE SUPREME PEOPLE'S COURT OF THE PEOPLE'S REPUBLIC OF CHINA, (Jan. 26, 2006, 9:01 AM), http://en.chinacourt.org/ public/detail.php?id=3992.

221. *Enforcement of Civil Judgments: Harder than Reaching the Sky*, CHINA L. AND GOVERNANCE REV. 10, 10 (June 2004), *available at* http://www.chinareview.info/PDFs/Issue%20No%202%20.pdf.

222. Daniel C.K. Chow, *Enforcement Against Counterfeiting in the People's Republic Of China*, 20 NW. J. INT'L L. & BUS. 447, 466–67 (2000). *See* Robert Bejesky, *Investing in the Dragon: Managing the Patent Versus Trade Secret Protection Decision for the Multinational Corporation in China*, 11 TULSA J. COMP. & INT'L L. 437, 455 (2004).

223. Chow, *supra* note 221, at 467.

224. *Id*.

225. Berkman, *supra* note 215, at 26–31 (1996).

226. *See* Shavell, *supra* note 120, at 364.

B. Three Concerns Relating to Regulation of Copyright Infringement in China

There are at least three major concerns relating to regulation of copyright infringement in China. First, government regulation may have an incredible chilling effect on speech. Second, it can lead to national favoritism. The government may do a lot to enforce the rights of Chinese content owners but do very little to enforce those of foreigners. The Chinese government has a record of such selective enforcement.[227] A third and related problem is rent seeking or corruption. Private parties may pay the government to turn a blind eye to their copyright infringements. Such rent seeking may be widespread.

1. A Chilling Effect on Speech

First, government regulation may have an incredible chilling effect on speech.[228] Three issues need to be addressed: first, whether benefits of anonymity outweigh its costs; second, whether a lack of anonymity has a serious chilling effect on speech; and third, whether government regulation has a greater chilling effect on speech than ISPs' monitoring, since ISPs have already engaged in invasive monitoring and have threatened anonymity.[229]

If subscribers know that the government monitors the Internet and regulates copyright infringement, they may be hesitant to express their ideas fully.[230] The amount of expression may diminish even before government regulation actually occurs.[231] Thus, government regulation of copyright infringement may create a disincentive toward robust expression.[232] Privacy advocates expressed concerns about legislative attempts that would require ISPs to retain subscribers' data.[233] People may tolerate occasional surveillance by police, but may not expect the government to record their daily routine in an unbroken stream.[234]

a. Cost-Benefit Analysis of Anonymity on the Internet

Anonymity is different from privacy, which usually covers a wide range

227. *See generally* Kristi Heim *Chinese Lawyer Talks Trade, Investment in Washington State*, SEATTLETIMES.COM (Aug. 31, 2010, 2:08 PM), http://seattletimes.nwsource.com/html/businesstechnology/2012764678_duanqa31.html (discussing the progress of intellectual property in China).

228. Christian M. Halliburton, *Letting Katz Out of the Bag: Cognitive Freedom and Fourth Amendment Fidelity*, 59 HASTINGS L.J. 309, 328–29 (2007) (discussing "the chilling effect that is associated with government restrictions on speech under First Amendment analysis."). *See* John Alan Farmer, Note, *The Specter of Crypto-Anarchy: Regulating Anonymity-Protecting Peer-To-Peer Networks*, 72 FORDHAM L. REV. 725, 729–31 (2003).

229. Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1423–24 (2009).

230. Halliburton, *supra* note 227, at 328–29.

231. *Id*.

232. *Id*. at 328.

233. *See* Anne Broache, *Attorney General to Talk Data Retention with New Congress*, CNET NEWS (Jan. 18, 2007, 2:49 PM), http://news.cnet.com/2100-1036_3-6151325.html.

234. Renée McDonald Hutchins, *Tied Up In* Knotts*? GPS Technology And The Fourth Amendment*, 55 UCLA L. REV. 409, 455 (2007).

of topics including movement, personal property, and information.[235] Anonymity can be regarded as "the perfect realization, or product of, privacy."[236] Having privacy does not necessarily make you anonymous, but being anonymous means that you have some form of privacy.[237] Thus, privacy is a prerequisite to achieving anonymity.[238]

Technological constraints in the past made it very difficult for the government to constantly monitor people's activities. The public could express ideas and keep their identities secret by avoiding the police. The development of information technology, however, enables the government to police online speech and activities easily and systematically. "[L]imited surveillance of activities visible to the public would most likely not trigger [anonymity] protection, but a more systematic campaign of public surveillance might present a different situation."[239] A commentator notes that "a violation of [anonymity] might occur if law enforcement authorities read private writings that were shared with a small group of people, but not with the public at large."[240] Even if the writing is shared with the public at large, a subscriber may expect anonymity because members of the public are normally unable to recognize his identity. It is similar to the situation in a bar where people generally expect anonymity among strangers.[241] If the government monitors the writing, an individual may fear losing anonymity and be restrained from expressing freely.

---

235. Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 300–301 (2001).

236. *Id.* at 301. Joseph Rosenbaum has attempted to divide privacy into three categories:

> "1. Territorial Privacy: one's right to be physically left alone or undisturbed. Territorial privacy is exemplified in the legal principles of trespass, real estate, and national sovereignty. This view of privacy allows one to impose physical boundaries around one's proprietary space to avoid the interference of other people or their effects.
>
> 2. Personal or Individual Privacy: one's right to be free in movement and expression without either physical assault or harassment in a non-physical sense (e.g., sexual harassment, defamation, obscenity). This type of privacy is based on social and cultural norms, and is tied to the individual's perceived sense of dignity rather than concepts of property. Laws concerning stalking, obscenity, and discrimination are related to this privacy category.
>
> 3. Information Privacy: one's right to protect dignity or integrity by preventing the disclosure, distribution, use, and abuse of information about oneself. This category of privacy is based on the idea that an individual has the exclusive right to disclose, communicate, control, or retain as private or public his personal information. People desire control over their personal information, allowing its disclosure to some and not to others, thus enabling citizens to govern their personal interactions. This category of privacy has been the focus of much attention due to recent advancements in the areas of database and data warehouse technology, in conjunction with the proliferation of the Internet. As a result, this type of privacy is also called 'database privacy."

Id. at 300–01 n.75 (citing Joseph I. Rosenbaum, *Privacy on the Internet: Whose Information Is It Anyway?* 38 JURIMETRICS J. 565, 566–67 (1998)). *See also* Rod Dixon, *Pledging to God While Getting a Public Education: Why a Wall of Separation Divides Ceremonial Celebration from Religious Indoctrination:* Elk Grove Unified School District v. Newdow *and the Right of Parental Privacy*, 48 J. CATH. LEG. STUD. 147, 194 (2009) (discussing three types of privacy: "(1) a physical aspect capable of invasion of space or self, (2) an informational aspect capable of invasion through unauthorized disclosure, and (3) a decisional aspect capable of invasion by force of authority, technological fiat, or formal and informal power").

237. Helms, *supra* note 234, at 301.

238. *Id.*

239. Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 157 (2007).

240. *Id.* at 157; Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups*, 46 ARIZ. L. REV. 621, 625–26 (2004).

241. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 238 (2002).

A commentator lists five private benefits of anonymity.[242] First, "the author may derive some internal, noninstrumental satisfaction from speaking without attribution."[243] It is similar to the moral right of attribution, which includes a right to be properly attributed as the author of what he has created, a right not to be attributed as the author of what he has not created, and a right to publish anonymously or under a pseudonym.[244] Second, anonymity may reduce "the potentially negative personal consequences of speaking truthfully."[245] This is referred to as the "Wrongful Retaliation" rationale.[246] For example, whistleblowers who report on government or corporate scandal may wish to remain anonymous to avoid possible retaliation.[247] Third, anonymity may reduce the private costs resulting from speaking falsely.[248] A discontented student may want to spread lies about his professor with impunity.[249] This is referred to as the "Justifiable Retaliation" rationale.[250] Fourth, anonymity may entitle the author to some collateral benefit at a lower cost.[251] For example, writers may publish favorable reviews of their own works anonymously.[252] Fifth, anonymity may increase the credibility and value of an author's speech.[253] One may be perceived by the public as untruthful or the supplier of low-quality work, but is in fact telling the truth or producing high-quality work.[254] Anonymity may prevent the public from underestimating the truth-value of his speech.[255]

A commentator lists two concerns relating to anonymity.[256] First, accountability may be missing because of anonymity.[257] Without accountability, more defamatory and false information will appear.[258] There is no way for an injured party to seek remedies. Anonymity also "seems to strip users of the civility that the face-to-face encounter has engendered in most modern societies."[259] Second, moving toward anonymity results in a loss of knowledge.[260] The analysis of personal information boosts innovation, assists

242. Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537, 1568 (2007).

243. *Id.*

244. *Id.* at 1568–70.

245. *Id.* at 1570–71.

246. *Id.* at 1568.

247. *Id.* at 1571.

248. *Id.* at 1568.

249. *Id.* at 1574.

250. *Id*.

251. *Id*. at 1568.

252. *Id*. at 1576.

253. *Id*. at 1577.

254. *Id*.

255. *Id*.

256. Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991, 1027–28 (2004).

257. *Id.* at 1028.

258. Ann Wells Branscomb, *Anonymity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1645 (1995); Zarsky, *supra* note 255, at 1028.

259. Branscomb, *supra* note 257, at 1645. *See* Lee Sproull & Sara Kiesler, *Computers, Networks, and Work*, *in* SOCIAL ISSUES IN COMPUTING: PUTTING COMPUTING IN ITS PLACE 335, 338–39 (Chuck Huff & Thomas Finholt eds., 1994).

260. Zarsky, *supra* note 255, at 1028.

startup ventures, and creates value.[261] Anonymity may make it impossible to collect private behavior data and disappoint some business entities which can otherwise innovate and create value with those data.[262]

Although anonymity may magnify the likelihood of false and abusive speech, traditional First Amendment theory provides two important premises: "[F]irst, that audiences are capable of rationally assessing the truth, quality, and other characteristics of core speech, and second, that more speech is generally preferable to less."[263] The Supreme Court of the United States noted clearly in *Dennis v. United State*s: "[T]he basis of the First Amendment is the hypothesis that speech can rebut speech, propaganda will answer propaganda, free debate of ideas will result in the wisest governmental policies."[264] In sum, the benefits of anonymity seem to outweigh its costs.

Commentators note that, however, it is uncertain that such a right to anonymity could even apply to the Internet.[265] In *Reno v. ACLU*,[266] "the Supreme Court found no basis for qualifying First Amendment rights [applicable] to speech on the Internet."[267] Lee Tien argues that a right to anonymity should translate to the Internet because "the Internet represents a

261. Tal Z. Zarsky, *Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society*, 56 ME. L. REV. 13, 33–38 (2004).

262. Zarsky, *supra* note 255, at 1028.

263. Lidsky & Cotter, *supra* note 241, at 1581. *See* Benjamin L. Liebman, *Scandal, Sukyandaru, and Chouwen*, 106 MICH. L. REV. 1041, 1046 (2008) ("Scandals on less sensitive topics, such as celebrity misconduct, are permitted to run, sometimes for extended periods, without official intervention."). *But see* Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 927–28 (2006) (challenging the presumption that "the public receives and reacts in a rational and predictable way to government information disclosed by the state."). Although there is censorship in China, such censorship is mostly limited to politically sensitive information. Citizens still have significant freedom of speech as to other types of content. Thus, the general theory of the First Amendment should apply to China.

264. Dennis v. U.S., 341 U.S. 494, 503 (1951).

265. Gayle Horn, *Online Searches and Offline Challenges: The Chilling Effect, Anonymity and the New FBI Guidelines*, 60 N.Y.U. ANN. SURV. AM. L. 735, 771 (2005). *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 337 (1995); George F. du Pont, *The Time Has Come for Limited Liability for Operators of True Anonymity Remailers in Cyberspace: An Examination of the Possibilities and Perils*, 6 J. TECH. L. & POL'Y 175, 178–79 (2001) ("[A] compromise between the need for remailers and the need to catch criminals must be reached. Such a compromise must reflect a realistic, good faith attempt to catch first-time abusers, while at the same time enabling truly anonymous, easily-accessible remailers to exist.").

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

267. Jason A. Martin, Mark R. Caramanica, & Anthony L. Fargo, *Anonymous Speakers and Confidential Sources: Using Shield Laws When They Overlap Online*, 16 COMM. L. & POL'Y 89, 93 (citing Shaun Spencer, *Cyberslapp Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace*, 19 J. MARSHALL J. COMPUTER & INFO. L. 492 (2001). *See* Joshua Furman, *Cybersmear or Cyber-SLAPP: Analyzing Defamation Suits Against Online John Does as Strategic Lawsuits Against Public Participation*, 25 SEATTLE U. L. REV. 213 (2001); Orit Goldring & Antonia L. Hamblin, *Think Before You Click: Online Anonymity Does Not Make Defamation Legal*, 20 HOFSTRA LAB. & EMP. L. J. 383 (2003); Noah Levine, Note, *Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV. 1526 (1996); Jenifer O'Brien, *Putting a Face to a (Screen) Name: The First Amendment Implications of Compelling ISPs to Reveal the Identities of Anonymous Internet Speakers in Online Defamation Cases*, 70 FORDHAM L. REV. 2745 (2002); Michael Vogel, *Unmasking "John Doe" Defendants: The Case Against Excessive Hand-Wringing Over Legal Standards*, 83 OR. L. REV. 795 (2004). *See also Reno*, 521 U.S. at 870 (discussing whether First Amendment is not applicable to some internet material); Victoria Smith Ekstrand, *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, 8 COMM. L. & POL'Y 405, 413–16 (2003). *But see, e.g.*, Ashcroft v. Free Speech Coal., 535 U.S. 234 (2002) (discussing the CPPA's effect on speech and child pornography); Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088. 1097 (W.D. Wash. 2001) (discussing First Amendment protections extending to the internet).

form of 'cheap speech' similar to leafleting or pamphleting."[268] He notes the differences between physical communication and online communication.[269] Being capable of hosting a large number of listeners from many places, the Internet has a stronger amplifying effect than TV or print.[270] Online anonymity "makes it easier to spread wild conspiracy theories, smear people, conduct financial scams or victimize others sexually."[271] Unlike online communication, pamphlets and telephone calls can be sent, but cannot cheaply and easily be "broadcast" on a large scale.[272]

In addition, the harm caused by a right to anonymity may be magnified because Internet communication is "global, instantaneous, and infinitely reproducible."[273] The sources of the speech, as well as the speech itself, have been amplified by the Internet.[274] Traditional wisdom about the freedom of speech assumes that the institutional press, which depends on the support of readers, would strive to achieve objectivity and balance to a certain extent.[275] The assumption does not apply to ordinary Internet users, however.[276] The Internet enables people to select and publish information more easily, where the audience not only reads a posting, but also shapes the message by interacting with each other over the Internet.[277] End users are amateurs, who do not need to please advertisers or readers, or are constrained by any journalistic or editorial ethics.[278] The problems inherent in a right to anonymity may be magnified, such as the lack of accountability that is caused by anonymous speech and the potential harassment to individuals because of that lack of accountability.[279]

Anonymity is not absolute. Lawmakers balance security and anonymity when deciding whether to enact an anonymity-enhancing regulation.[280] Paul Ohm notes the lack of discussion about opposing values such as security in some of the most interesting and important recent works about data privacy.[281] In Professor Julie Cohen's important early work on online privacy, she spends very little time on weighing interests offsetting privacy, concluding with little discussion at one point that "[t]he baseline presumption should be one of strong data privacy protection; exceptions should be carefully considered and narrowly circumscribed."[282] Because the arguments in favor of anonymity are

268. Horn, *supra* note 264, at 771 (citing Lee Tien, *Who's Afraid of Anonymous Speech?* McIntyre *and the Internet*, 75 OR. L. REV. 117, 136–39 (1996)).

269. Tien, *supra* note 267, at 151–54.

270. *Id*. at 151–52.

271. Branscomb, *supra* note 257, at 1645 n.19 (citation omitted).

272. *But see* Tien, *supra* note 267, at 151–52.

273. John Alan Farmer, *The Specter of Crypto-Anarchy: Regulating Anonymity-Protecting Peer-To-Peer Networks*, 72 FORDHAM L. REV. 725, 774 (2003).

274. *But see* Tien, *supra* note 267, at 152.

275. *Id*.

276. *Id*.

277. Horn, *supra* note 264, at 771–72.

278. *See* Tien, *supra* note 267, at 152.

279. Horn, *supra* note 264, at 772.

280. Ohm, *supra* note 228, at 1462–63.

281. *See id.* "Data privacy" and "anonymity" are used interchangeably for the purpose of this article.

282. Julie Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1432 (2000); Ohm, *supra* note 228, at 1463.

abstract, they are unlikely to influence lawmakers.[283]

b. ISPs' Invasive Monitoring and Government Regulation

ISPs have already engaged in invasive monitoring and have threatened anonymity. If a right to anonymity should be applied to the Internet, will government regulation have a more serious chilling effect on speech than ISP surveillance?

ISPs have been monitoring end users' activities in two ways.[284] First, they use automated computer programs to scrutinize all the packets transmitted in a network for problematic communications.[285] When ISPs suspect problems, they will deploy a targeted tool, called a packet sniffer, to deeply inspect packets and record everything it finds.[286] A mixture of automated and targeted monitoring did not raise a serious privacy concern in the past.[287] Automated monitoring does not invade privacy because almost all of the private details are removed before humans see them.[288] Targeted monitoring does not seriously threaten privacy either because it is rare or temporary.[289]

These days, however, ISPs have monitored users' communication more invasively than before for three reasons.[290] First, new Internet applications, such as P2P file sharing, force ISPs to upgrade the network infrastructure and increase bandwidth without charging end users a higher fee.[291] As a result, the revenue earned per bit is eroded at an accelerating pace.[292] Network management of illicit copyrighted content reduces congestion and avoids additional costs of upgrading the infrastructure. It is estimated that up to 70% of broadband bandwidth is consumed by music, movies, games, and similar unproductive downloads.[293] The consequence is that either through new

283. Ohm, *supra* note 228, at 1463–64 (examining whether privacy-invading monitoring is necessary).
284. *Id.* at 1424.
285. *Id.*
286. *Id.*
287. *Id.* at 1425.
288. *Id.* at 1424–25.
289. *Id.*
290. *Id.* at 1425–26; Louise Story, *A Company Promises the Deepest Data Mining Yet*, N.Y. TIMES, Mar. 20, 2008, at C3 (reporting that Phorm "has created a tool that can track every single online action of a given consumer, based on data from that person's Internet service provider"). *See also* Ernesto, *Comcast Throttles BitTorrent Traffic, Seeding Impossible*, TORRENTFREAK (Aug. 17, 2007), http://torrentfreak.com/comcast-throttles-bittorrent-traffic-seeding-impossible/ (reporting that Comcast prevented BitTorrent users from seeding); Marguerite Reardon, *Should AT&T Police the Internet?*, CNET, (Jan. 17, 2008, 4:00 AM), http://news.cnet.com/Should-ATT-police-the-Internet/2100-1034_3-6226523.html ("AT&T executives have said the company is testing technology to filter traffic on its network to look for copyrighted material that is being illegally distributed.").
291. Ohm, *supra* note 228, at 1425–26.
292. *Deep Packet Inspection: Vendors Tap into New Markets*, HEAVY READING INSIDER, http://www.lightreading.com/insider/details.asp?sku_id=1974&skuitem_itemid=1060 (last visited Sept. 28, 2011). *See also* DELOITTE TOUCHE TOHMATSU, TECH., MEDIA, & TELECOMM. GRP., TELECOMMUNICATIONS PREDICTIONS: TMT TRENDS 2007 at 7, *available at* http://www.deloitte.com/assets/Dcom-Bulgaria/Local%20Assets/Documents/bg_tmt_predictions_2007_telecoms.pdf ("ISPs and telecommunications carriers are seeing revenues stagnate. As penetration growth slows, competition drives down prices and rapidly rising Internet use among existing customers erodes margins.").
293. *Managing Peer-to-Peer Traffic with Cisco Service Control Technology*, CISCO SYS., http://www.cisco.com/en/US/prod/collateral/ps7045/ps6129/ps6133/ps6150/prod_white_paper0900aecd8023500d.html (last visited Sept. 29, 2011).

business models or through the added expenses of constantly upgrading their networks, ISPs will face economic pressures to enforce copyright. Inspired by Google's success, ISPs have begun to explore new sources of revenue by displaying advertisements matching a user's private behavior data such as web transfers, instant messages, and e-mail messages.[294] In other words, ISPs have started to trade user privacy for revenue.

Second, ISPs have engaged in invasive monitoring as a result of outside pressures from the government and copyright owners.[295] In 1994, the Communications Assistance for Law Enforcement Act (CALEA) was passed due to the lobbying efforts of the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI).[296] Under CALEA, ISPs are required to "configure their networks to be able quickly to assist law enforcement monitoring" under limited conditions.[297] In addition, the recording and motion picture industries have exerted significant pressure on ISPs to monitor users' copyright infringement.[298] ISPs, such as Comcast, AT&T, and EarthLink, may be obliged to sniff digital packets, searching for content that may infringe someone's copyright.[299]

Third, all the major ISPs who provide Internet access are also incumbent content disseminators whereas, in the early days of the Internet, ISPs and the copyrighted content providers were different entities. The top ISPs in the United States include AT&T, Comcast, Verizon, Time Warner Cable, and Cox, all of which deliver content in addition to providing Internet access. The programming market is also highly concentrated, with disseminators owning programmers.[300] For example, Time Warner Cable is affiliated with Time-Warner, Inc., a major producer of copyrighted content. This trend will continue if the proposed Comcast-NBC Universal merger is approved. The ISP Comcast is now a superpower controlling both dissemination and copyrighted content through its subsidiary NBC Universal.[301]

---

294. Ohm, *supra* note 228, at 1425–26; Raymond McConville, *Telcos Show Their Google Envy*, LIGHT READING (Apr. 8, 2008), http://www.lightreading.com/document.asp?doc_id=150479&f_src=lightreading_FinancialContent (referencing the need for ISPs to open themselves up to third-party advertising).

295. Ohm, *supra* note 228, at 1426–27.

296. *Id*.

297. *Id*. at 1427.

298. Anne Broache, *RIAA: No Need to Force ISPs by Law to Monitor Piracy*, CNET (Jan. 30, 2008 12:50 PM) http://news.cnet.com/8301-10784_3-9861460-7.html (noting that Recording Industry Association of America's President Cary Sherman said that "he was encouraged to see that some companies, such as AT&T, are already experimenting with network filters."); Ohm, *supra* note 228, at 1426–27.

299. Brad Stone, *AT&T and Other I.S.P.'s May Be Getting Ready to Filter*, N.Y. TIMES (Jan. 8, 2008 7:07 PM), http://bits.blogs.nytimes.com/2008/01/08/att-and-other-isps-may-be-getting-ready-tofilter/.

300. Marvin Ammori, *Copyright's Latest Communications Policy: Content-lLock-Out & Compulsory Licensing for Internet Television*, 18 COMMLAW CONSPECTUS 375, 381 (2010).

301. *Id*. at 381–87. *See also* Ian Paul, *NBC-Universal-Comcast Merger: What We Do & Don't Know*, PCWORLD (Dec. 3, 2009, 1:40 PM), http://www.pcworld.com/article/183652/nbcuniversalcomcast_merger_what_we _do_and_dont_know.html (listing potential content providers as "NBC Television Network; specialty channels including USA, Bravo, CNBC, MSNBC, Syfy, E!, Style, Versus and the Golf Channel; Universal Pictures and Universal Studios Home Entertainment; local broadcast TV stations in ten top U.S. markets including New York, Los Angeles, Chicago and Philadelphia; the national Telemundo Network and 16 Telemundo owned-and-operated stations in locations such as Los Angeles, New York, Miami, Houston, Chicago and Dallas/Ft.Worth; NBC Universal Domestic and International Distribution and a 3,000-title library of television episodes; NBC News including Nightly News with Brian Williams, the Today show and Meet the Press; rights to sports programming including the Olympics (through 2012), NBC Sunday Night Football,

The public assumes that surveillance is harmful to some degree. Many dislike being followed by others, or simply feel uncomfortable that the government or a private party knows so many details about them.[302] The assumption of harm, however, lacks adequate basis. A commentator notes that:

> At this point, however, there is insufficient research to convincingly demonstrate that constant surveillance amounts to a form of regulatory harm. It must be shown that the networked environment actually prevents or substantially discourages speakers and assemblies from engaging in public expressive activities. Even with such a showing, however, the government's response will likely be that the threat of terrorism and other criminal activity is a compelling reason to put public areas under surveillance. Indeed, that concern has already caused some courts to loosen restrictions on political surveillance.[303]

In fact, a danger of inappropriate disclosure of personal information, rather than surveillance, may have a chilling effect on speech.[304] A commentator notes that "if the user is confident that the information gathered will be used only as a marketing tool, she is unlikely to modify her behavior in light of the surveillance. There will only be a serious threat to privacy if there is a danger of inappropriate disclosure of personal information."[305] Although an ISP has already undertaken invasive monitoring, it has a record of respecting privacy.[306] Maybe that is why the ISP monitoring has not had a serious chilling effect on speech so far. But can we also assume that government surveillance is alright if the government avoids inappropriate disclosure?

A commentator distinguishes videotaping by a private party from that by the government.[307] First, while it is difficult for a private party to place cameras throughout a city's streets, the government is able to create an inescapable video surveillance system.[308] Second, the government may integrate the collected information into its comprehensive database and do more harm to individuals than a private party does.[309] The government use or misuse of the data is likely to chill speech. Another commentator notes that "surrendering identifying information to governmental authorities is qualitatively different from giving a name to some private party (a marketer,

---

NHL/Stanley Cup, PGA Tour, US Open, Ryder Cup, Wimbledon and the Kentucky Derby, Versus, Golf Channel and Comcast's 10 regional sports networks; digital properties including CNBC.com, Daily Candy, iVillage and Fandango; ownership of theme parks in Florida (50% interest), California (100% interest) and a financial interest in a theme park in Japan; minority interest in A&E, Biography, The History Channel, The Weather Channel, Lifetime and Hulu.com.").

302. Ravine, *supra* note 13, at ¶¶ 6–7.

303. Timothy Zick, *Clouds, Cameras, and Computers: The First Amendment and Networked Public Places*, 59 FLA. L. REV. 1, 38 (2007).

304. Ravine, *supra* note 13, at ¶ 6.

305. *Id*.

306. Ohm, *supra* note 228, at 1446–47.

307. Marc Jonathan Blitz, *Video Surveillance & The Constitution Of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1431–33.

308. *Id*.

309. *Id.* at 1432.

new acquaintance, etc.)."[310]

> [T]he Government has the capacity to use your name or other nonpublic identifying information to access unparalleled amounts of personal information. The Court has indicated that while the use of technology to enhance investigatory capabilities does not automatically establish a search, it is more likely that a search has occurred within the meaning of *Katz* when that technology is "not in general public use" and circumvents the protections of the Fourth Amendment. The informational databases available to governmental authorities in conducting background checks are not in general public use. Although it will be pointed out that the personal information is already stored with various governmental agencies before police officers obtain a suspect's name, merely possessing personal information is significantly different from linking that information to a name and face.[311]

Whether or not inappropriate disclosure of personal information occurs, government surveillance seems to have an inevitable chilling effect on speech because the government can access various informational databases and enforce the law. The Chinese government, however, has been regulating the Internet for a long time by filtering online content.[312] Thus, imposing on the Chinese government an additional task of deterring online copyright infringement should not have a more serious chilling effect on speech.

2. National Favoritism

Regulation can lead to national favoritism. The government may do a lot to enforce the rights of Chinese content owners but do very little to enforce those of foreigners. The Chinese government has a record of such selective enforcement.[313] In fact, foreign works enjoyed "super-national treatment" in China before 2001.[314] After China acceded to international conventions, specifically the Berne Convention and the Universal Copyright Convention, there were significant discrepancies between the 1990 Copyright Law and international conventions.[315] As a result, the State Council drafted a special administrative act to protect the interests of foreign nationals according to international conventions.[316] The consequence is that foreign nationals under international conventions enjoyed superior treatment than Chinese nationals, which impaired the development of a competitive market.[317] Although the

310. Estrada, *supra* note 14, at 305.

311. *Id.*

312. *See supra* text accompanying notes 196–210 (discussing internet filtering).

313. *See* Jared A. Berry, Note, *Anti-Monopoly Law in China: A Socialist Market Economy Wrestles with Its Antitrust Regime*, 2 INT'L L. & MGMT. REV. 129, 146 (2005) (discussing China's use of anti-monopoly laws to prevent dominance of foreign corporations).

314. Xiaoqing Feng & Frank Xianfeng Huang, *International Standards and Local Elements: New Developments of Copyright Law in China*, 49 J. COPYRIGHT SOC'Y U.S.A. 917, 919 (2002).

315. *Id*.

316. *Id*.; [Provisions on the Implementation of the International Copyright Treaties] (promulgated by the St. Council, Sept. 25, 1992, effective Sept 30, 1992), *translation available at* http://www.worldlawdirect.com/article.php?id=3139 (English version of Chinese full text regulation).

317. Feng & Huang, *supra* note 313, at 919.

2001 Copyright Law eliminated the "super-national treatment,"[318] foreign copyright owners do not need to worry about the government's selective enforcement, because they can easily monitor online copyright infringement and bring actions against the government for its selective enforcement.[319] Unable to risk promotion and bonus, government officials will have to take action against copyright infringement.

3. Rent Seeking or Corruption

A third and related problem is rent seeking or corruption. Private parties may pay the government to turn a blind eye to their copyright infringements.[320] Such rent seeking may be widespread. There are two types of rent seeking: the government may choose not to prosecute the infringer or may choose to prosecute the innocent.[321] A commentator notes the causes of corruption:

> Some circumstances facilitate corruption. A key determinant is the reward structure. Bureaucratic traditions that favour recruitment or promotion of officials on arbitrary grounds, as opposed to on the merits, and low salary levels are part of this. Another determinant is the effectiveness of accountability systems. Lack of transparency, discretionary powers for officials, and room for arbitrary decisions impede accountability. The low probability of being exposed and lenient consequences for an official, who does get caught, are also part of an inadequate accountability system. A third factor is the leadership. Corruption will thrive in the absence of political leadership that is strongly committed to anti-corruption activities.[322]

Because prosecutors have discretion in determining whether to prosecute a criminal suspect, it would be helpful to examine how the government deals with rent-seeking prosecutors. Some enforceable laws set the boundaries of prosecutorial discretion.[323] Public oversight also bounds prosecutorial discretion, as a commentator notes:

> The other main remedy for prosecutorial misconduct [besides administrative supervision, trial court control, and appellate review] is public oversight. State district attorneys typically are elected officials. Misconduct within their offices-even by lawyers whom they have not directly supervised- becomes an issue during elections. Accordingly,

---

318. [Copyright Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Sept. 7, 1990, revised Oct. 27, 2001), *translation available at* http://www.wipo.int/wipolex/en/text.jsp?file_id=125980 (English version of Chinese full text regulation) [hereinafter Copyright Law of China].

319. *Id.*

320. *See* Claes Sandgren, *Combating Corruption: The Misunderstood Role of Law*, 39 INT'L LAW. 717, 725 (2005) (explaining how and why payment of public officials occurs in various contexts).

321. *Cf.* Keith N. Hylton & Vikramaditya Khanna, *A Public Choice Theory of Criminal Procedure*, 15 SUP. CT. ECON. REV. 61, 84–87 n.81 (2007) (explaining rent seeking where prosecutors accept bribes not to enforce charges). *See generally* Rebecca A. Pinto, *The Public Interest and Private Financing of Criminal Prosecutions*, 77 WASH. U. L.Q. 1343, 1353 n.50 (1999); Jeffrey Standen, *An Economic Perspective on Federal Criminal Law Reform*, 2 BUFF. CRIM. L. REV 249, 261–68 (1998).

322. Sandgren, *supra* note 319, at 725.

323. Bruce A. Green & Fred C. Zacharias, *Prosecutorial Neutrality*, 2004 WIS. L. REV. 837, 846–47 (2004).

> media attention and political review by the voters may provide a deterrent or, at least, a reason for district attorneys to take corrective steps when misconduct is brought to their attention.[324]

Confidentiality is one of the conditions to facilitate corruption.[325] Unlike nontransparent administrative approval, online copyright infringement is much easier to monitor, even without the help of media. Corruption in copyright enforcement in China is difficult to hide and is likely to be deterred by public oversight.[326]

Despite corruption, regulation can be an appealing approach in dealing with copyright infringement outside the judicial system.[327] An article discusses the optimal law enforcement with a rent-seeking government and advocates competitive private enforcement.[328] Private monitoring avoids many of the above problems. In the long run, it is quite likely that private parties will be able to monitor copyright infringement at a lower cost. Furthermore, competition in the detection industry may develop over time.[329] The

---

324. Carolyn B. Ramsey, *The Discretionary Power of "Public" Prosecutors in Historical Perspective*, 39 AM. CRIM. L. REV. 1309, 1320 (2002). *See also Criminal Law Comes Home*, 116 YALE L.J. 2, 45 (noting that "prosecutors make decisions in the shadow of public oversight and have an enhanced incentive to use every means available to protect victims"). *But see* Rachel E. Barkow, *Institutional Design and the Policing of Prosecutors: Lessons from Administrative Law*, 61 STAN. L. REV. 869, 911 (2009); Samuel W. Buell, *The Upside of Overbreadth*, 83 N.Y.U. L. REV. 1491, 1554 n.252 (2008) ("[W]hile efforts to increase legislative and public oversight over prosecutors sound promising on paper, they cannot serve as a realistic check in today's political climate."); Ramsey, *supra* note 323, at 1320 (opposing the idea that "the honorable prosecutor be the slave of his electorate").

325. *See* SUSAN ROSE-ACKERMAN, CORRUPTION AND GOVERNMENT: CAUSES, CONSEQUENCES, AND REFORM 162–74 (1999) (discussing the need for openness to prevent corruption in government); Edgardo Buscaglia & Maria Dakolias, *An Analysis of the Causes of Corruption in the Judiciary*, 30 LAW & POL'Y INT'L BUS. 95, 100 (1999) (noting the five reasons for corruption: "(1) a higher concentration of internal organizational roles concentrated in the hands of fewer decision makers within a public agency. . . (2) the added number and complexity of the procedural steps coupled with a lack of procedural transparency followed within a government agency supplying a service. . . (3) the greater uncertainty related to the prevailing doctrines, laws, and regulations. . . (4) fewer alternative sources of the good or service demanded from the government. . . and (5) the lack of collusive behavior found among the parties demanding a legal or illegal service from a public agent or agency"); Nicholas Miranda, *Concession Agreements: From Private Contract to Public Policy*, 117 YALE L.J. 510, 521 n.44 (noting the three key causes of corruption identified by the World Bank: "lack of institutional restraints, lack of transparency of actors, and lack of general accountability"); Daniel Treisman, *The Causes of Corruption: A Cross-National Study*, 76 J. PUB. ECON. 399, 436 (2000). *See OverviewAnti-Corruption*, WORLD BANK, http:// http://go.worldbank.org/K6AEEPROC0 (last visited Sept. 21, 2011) (listing the streghtening of civil participation as one of five factors to an effective anti-corruption strategy). *See also* David Hess & Cristie L. Ford, *Corporate Corruption and Reform Undertakings: A New Approach to An Old Problem*, 41 CORNELL INT'L L.J. 307, 315–16 (2008) ("Solving the problem of corruption requires that it be attacked with a variety of approaches that simultaneously address different causes of the problem. These approaches must seek to both reduce the demand for bribes (which comes from public officials receiving the bribes) and restrict the supply (which comes from corporations paying the bribes)."); Vito Tanzi, *Corruption Around the World: Causes, Consequences, Scope, and Cures*, 45 IMF STAFF PAPERS 559, 569 (1998), *available at* http:// idari.cu.edu.tr/igunes/butce/makalebutce29.pdf (noting that in situations where officials "have discretion over important decisions . . . corruption, including high-level or political corruption, can play a major role").

326. *See* Buscaglia, *supra* note 324, at 100.

327. Jeffrey F. Levine, *Meeting the Challenges of International Brand Expansion in Professional Sports: Intellectual Property Right Enforcement in China Through Treaties, Chinese Law and Cultural Mechanisms*, 9 TEX. REV. ENT. & SPORTS L. 203, 220 (2007).

328. Nuno Garoupa & Daniel Klerman, *Optimal Law Enforcement with a Rent-Seeking Government*, 4 AM. L. & ECON. REV. 116, 116–117 (2002).

329. *See generally NEC Develops Video Content Identification Technology that Detects Illegal Copies in a Matter of Seconds*, PHYSORG.COM (May 7, 2010), http://www.physorg.com/news192458123.html *(demonstrating that companies are competing in the detection services market). See also Technology*

government on the other hand will remain a monopoly.

V. CONCLUSION

The Internet's precise and inexpensive distribution system provides copyright owners with new opportunities to profit from their works. Illicit use of their works, however, is becoming more difficult to deter because of the relative anonymity of cyberspace. Copyright owners have attempted unsuccessfully to solve the problem by holding ISPs liable for subscriber misconduct.

This article aims to solve the problem from a new angle—government regulation of online copyright infringement. The purpose of the article is to provide academics and policymakers with a consistent framework for evaluating the relative desirability of ISP liability and regulation of copyright infringement. By taking China as an example, I discuss the four determinants of the framework in detail. Because of the market distortion effect of ISP liability, government regulation may be an appealing alternative to prevent online copyright infringement. It is highly likely that policymakers will need to rely on this framework, while adapting it to novel infringements.

Overview, AUDIBLE MAGIC CORP. http://audiblemagic.com/products-services/contentsvcs/ (last visited Sept. 28, 2011). *About Us*, CIVOLUTION, http://www.civolution.com/home/ (last visited Sept. 28, 2011) (retailing audio technologies); *About Us*,; VOBILE INC., http://www.vobileinc.com/ (last visited Sept. 28, 2011) (retailing recent technologies).