

## On Compliance & Code: Does Peer-to-Peer Really Challenge Law?

Tim Wu<sup>1</sup>

### Introduction

When the Supreme Court upheld extended copyright terms in *Eldred v. Ascroft*,<sup>2</sup> many internet activists called for renewed political action: appeals to Congress, and even a campaign to amend the Constitution. But others suggested a very different course. They argued that it would be wiser to forgo institutions controlled by the powers of the past, and return, instead to the keyboard, to write the next generation of “law-busting” code. In the words of one observer, “tech people are probably better off spending their energy writing code than being part of the political process” for “[t]hat’s where their competitive advantage lies.”<sup>3</sup>

The idea that computer code may be emerging as a meaningful instrument of political will remains both the most evocative and poorly understood propositions in the study of law and technology. While many have come to accept that code may be, in Lessig’s phrase, an alternative modality of regulation,<sup>4</sup> we still have only the barest idea of what that means. The subject remains an area of rampant speculation, ranging from predictions that law is fading to irrelevance,<sup>5</sup> to claims that we face a future in which code underlies ever-increasing control over every aspect of life.<sup>6</sup> Both these accounts, meanwhile, can be contrasted with persistent claims that nothing of striking legal novelty has happened.<sup>7</sup>

---

<sup>1</sup> Tim Wu, Associate Professor of Law, University of Virginia School of Law. I am grateful to Jack Goldsmith, Scott Hemphill, Jody Kraus, Lawrence Lessig, Clarisa Long, Tom Nachbar, Irene Oh, Eric Posner, and Matthew Schruers for discussion and comments on earlier and much earlier drafts; to workshop participants at the 2002 Canadian Law & Economics Conference, the Stanford Law School Internet and Society Speaker Series, and to Miriam Cho and Kelly DeMarchis for research assistance.

<sup>2</sup> 123 S. Ct. 769 (2003).

<sup>3</sup> Declan McCullagh, Geeks in government: A good idea?, at <http://news.com.com/2010-1071-949275.html> (Aug. 12, 2000) (quoting Sonia Arrison of the Pacific Research Institute).

<sup>4</sup> See Lawrence Lessig, Code and Other Laws of Cyberspace 89 (1999).

<sup>5</sup> These claims are described and discussed in Timothy Wu, *When Law & The Internet First Met*, 3 GREEN BAG 2D 171, 172-173 (2000); cf. Tom W. Bell, Escape From Copyright: Market Success vs. Statutory Failure In The Protection Of Expressive Works, 69 U. Cin. L. Rev. 741 (2001) (arguing that efficacy of technological self-help should allow voluntary exit from the copyright regime).

<sup>6</sup> See Lessig, *supra* n. 4, at 213-221.

<sup>7</sup> See, e.g., Jim Septa, Internet Theology, 2 Green Bag 2d 227 (1999) (Arguing that internet publication does not justify major changes to 1st Amendment regime); Bruce P.

Problematically, none of these general theories does much to explain a central issue: compliance; specifically, the changes in pattern of compliance in the 2000s. Explosions of non-compliance in areas like copyright, pornography, financial fraud and prescription drugs fuel the sense of a legal breakdown. Yet the vast majority of laws remain unaffected. Today's focus on code as a substitute for law does little to explain why this mixed pattern exists.<sup>8</sup>

This Article proposes a new and more concrete way to understand the puzzle of code and compliance. I propose that we may best understand these questions by studying the effect code on interest group behavior. The design of code be described as an alternative *mechanism* that some regulated groups will use to influence law's effects. It can be in other words, understood as an alternative to a lobbying campaign or any other approach a group might use to influence law and its effects.

This perspective takes seriously the potential for code to undercut legal regimes. Yet when viewed this way it becomes obvious that as a mechanism of interest group influence, code design is of limited capacity.<sup>9</sup> Most prominently, it is a mechanism of *evasion* rather than a mechanism of *change*. It targets specific weaknesses in legal enforcement, rather than serving as a means to rewrite laws in general. Therefore, I argue that its

---

Keller, *The Game's The Same: Why Gambling In Cyberspace Violates Federal Law*, 108 *Yale L.J.* 1569 (1999) (arguing that internet gambling should be regulated as usual); Edward A. Morse, *State Taxation Of Internet Commerce: Something New Under The Sun?*, 30 *Creighton L. Rev.* 1113 (1997) (arguing that issues of state taxation of internet-based commerce are familiar). This view can also be attributed to Jack Goldsmith, though in his view, unfairly. See Jack L. Goldsmith, *Against Cyberanarchy*, 65 *U. Chi. L. Rev.* 1199 (1998).

<sup>8</sup> E.g., Bell, *supra* note 5; Lessig, *supra* note 4; Julie E. Cohen, *Lochner In Cyberspace: The New Economic Orthodoxy Of "Rights Management*, 97 *Mich. L. Rev.* 462 (1998) (challenging the attractiveness of technological self-help as substitute for legal regimes). Nor does the scholarship examining the metaphors used for internet conduct explain compliance patterns. See, e.g., Orin Kerr, *The Problem of Perspective in Internet Law*, 91 *Georgetown L. J.* (forthcoming 2003) (arguing that technological perspectives decide internet cases); Dan Hunter, *Cyberspace as Place*, 90 *Cal. L. Rev.* (forthcoming 2003) (noting the persistence of the space metaphor); Alfred C. Yen, *Western Frontier Or Feudal Society?: Metaphors And Perceptions Of Cyberspace*, 17 *Berkeley Tech. L.J.* 1207 (2002) (comparing metaphors of the frontier with cyberspace); Timothy Wu, *Application Centered Internet Analysis*, 85 *Virginia L. Rev.* 1163 (1999) (arguing that analysis should focus on application development).

<sup>9</sup> Importantly, this is claim relating only to code design as a mechanism of legal influence. It is not a claim about code's relevance in other respects; notably as an instrument of regulation, as detailed in Lessig, *supra* n. 4.

greatest long-term significance will lie in providing new options for individuals, and large, disorganized groups, not well disposed to take advantage of alternative means. But as a general matter, the design of code to circumvent laws will matter only for vulnerable laws: particularly, those lacking normative support and dependent on vulnerable supplemental enforcement structures.

The important case of peer-to-peer filesharing (P2P), explored in depth in this Article, gives concrete demonstration of these premises. These ingenious programs, bearing names like “KaZaa” and “Bearshare,” make it free and easy to trade digital content (usually copyrighted songs) with millions of new-found friends. The significance of P2P for copyright is real. The efforts of P2P programmers have provided computer-savvy music listeners with a continuing reduction in the costs of copyright, comparable to a temporary repeal of copyright for computer geeks. P2P underlines the reality of code design as an alternative mechanism of interest group behavior.

But P2P also makes the limits equally clear. First, P2P depends both on two powerful, and often unrecognized weaknesses of the copyright regime: the law’s dependence on a gatekeeper enforcement regime and severe lack of normative support among the regulated. It leaves the law stripped to primary enforcement against a multitude of end-users, a recognized area of weakness.

Second, P2P’s success may depend on a unique collective action dynamic among music consumers that stems from the nature of copyrighted works. The songs and other content available on peer networks are generally non-rivalrous goods.<sup>10</sup> As a result, P2P users, young and minimally computer-savvy,<sup>11</sup> can as a sub-group take advantage of the continued compliance of regular consumers. Ideally, the mass of regular users pay for works, creating incentives for their creation, while the P2P sub-group defects en masse, occupying the game-theorist’s version of utopia..

These specific weaknesses of copyright are not general weaknesses of the legal system. For that reason, the utility of P2P as an evasion mechanism beyond copyright appears limited. Other laws may contain other particularized enforcement weaknesses comparable to copyright’s, such as the

---

<sup>10</sup> That is to say, one individual’s consumption does not diminish another user’s value of the product. I mean this for the songs themselves some have suggested that songs on peer networks display rivalrous features. See Ramayya Krishnan, et al., *The Economics of Peer-To-Peer Networks* at 5 (August 2002 draft) available at <http://www.heinz.cmu.edu/~mds/>.

<sup>11</sup> According to an Ipsos-Reid study, those who use peer filesharing networks are predominantly between the ages of 12-24. See Robyn Greenspan, *Making Money on Free Music*, <http://www.internetnews.com/stats/article.php/1365161>

laws restricting pornography, the upshot is a mechanism of meaningful, yet limited potential.

\* \* \*

This Article's claims rely on a model of compliance and interest group behavior with certain novel features. Namely, the focus is on the mechanisms through which groups influence law. It is the goal of first part of the Article to make the underlying model clear.

Laws impose costs upon regulated groups. Those that seek to minimize the costs of law face a fundamental choice between mechanisms of *change* and *avoidance*. Both types of mechanism have the same effect of lowering the expected costs of law. But the similarities end there. Mechanisms of change (principally, lobbying) act to decrease the sanction attached to certain conduct for the long-term and tend to require collective action. Mechanisms of avoidance, on the other hand, decrease the probability of detection, and are typified by lacking a need for groups to act collectively, but depend of specific vulnerabilities in the law.

This understanding, while not exhaustive, is descriptively useful even in the simple form presented here. It shows the link of problems of compliance to group dynamics: how organized the regulated are. And it shows that changes in the costs of mechanisms of legal influence can dramatically effect the function of a given law.

Part II of this article demonstrates the very particular fit between the vulnerabilities of copyright and the design of code to exploit those weaknesses. Copyright enforcement has long relied on what Professor Reinier Kraakman first called a gatekeeper regime.<sup>12</sup> In other words, copyright has achieved its goals through enforcement against specialized intermediaries—those capable of distributing creative works on a mass scale. Peer networks exploit that enforcement structure by creating a distribution network that eliminates intermediaries. While eliminating intermediaries at a mass scale presents a serious technical challenge, the goal is clear—to remove the enforcement efficiency of a gatekeeper system, leaving primary enforcement only against end-users.

P2P also exploits an existing and powerful ambiguity over the ethics of home copying. Compliance with laws pertaining to the theft of real property is aided by clearly established norms. These norms helps prevent

---

<sup>12</sup> Reinier H. Kraakman, Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy, 2 J. L. Econ. & Org. 53, 53-54 (1986).

certain forms of economic injury to copyright owners, like the stealing of books or CDs from stores. Studies show that people are generally untroubled, by the non-commercial home copying of copyrighted content.<sup>13</sup> Peer filesharing are designed to create a distribution mechanism that looks and feels more like home copying, than breaking into a record store. The design therefore successfully exploits this normative distinction.<sup>14</sup>

Part III shows that P2P has grown through several iterations to specialize in the exploitation of copyright's gatekeeper system. By the end, the peer-to-peer story suggests real limits on the general utility of making use of network design to influence law. Influencing the law in such a manner requires, as the study shows, particular vulnerabilities in the law and a group that lacks better options. The limits in generalizing the peer-to-peer model to areas of law beyond copyright demonstrate why the compliance challenge is specific to certain classes of vulnerable laws, not a general challenge to the legal system.

Part IV of the paper concludes by studying the fit between P2P and music consumers as an interest group. A fascinating aspect of the peer filesharing story is the lack of coordination and organization attending its development. Developers bicker and work independently, and etiquette among users must be engineered or, as Lior Strahilevitz argues, induced with "charismatic code."<sup>15</sup> Despite the chaos, peer networks have managed to provide a subset of music listeners with a continuing reduction in the costs of copyright.

Such results from a disorganized efforts are consistent with the distinction between a mechanism of *avoidance* and opposed to *change*. It supports the claim that the long-term significance of code design for influencing law may be for groups whose inability to act collectively precludes better options.

Finally, the results may also reflect the current ability of P2P users, as a group, to take advantage of the continued compliance of the majority of the population. Copyright's subjects are divided by a technological line between the computer-savvy and regular users. Because consumption of copyrighted

---

<sup>13</sup> See Amanda Lenhart et al., Downloading Free Music: Internet music lovers don't think it's stealing, The Pew Internet & American Life Project's Online Music Report, Sept. 28, 2000, at 5, available at <http://www.pewinternet.org/reports/toc.asp?Report=23>; U.S. Congress, Office of Technology Assessment, Copyright and Home Copying: Technology Challenges the Law 163 (1989), available at [http://www.wss.princeton.edu/~ota/disk1/1989/8910\\_m.html](http://www.wss.princeton.edu/~ota/disk1/1989/8910_m.html).

<sup>14</sup> Cf. Lior Strahilevitz, Charismatic Code, Social Norms and the Emergence of Cooperation on the File-Swapping Networks, 89 Va. L. Rev (forthcoming 2003) (arguing that the charismatic code that creates an illusion of reciprocity accounts for why people contribute to a file-sharing network).

<sup>15</sup> See generally, id.

<sup>16</sup>

works is non-rivalrous, P2P users may rely on regular users to pay for music and provide incentives for its creation, free-riding on the results.

\* \* \*

Analyzing code design as a mechanism of interest group behavior yields a nuanced picture. It departs from the grandiose predictions that dominate discussion in this area. As with onset of lobbying, impact litigation, or sophisticated tax evasion, the potential to affect the law's effects should not be mistaken for an elimination of the legal system. Instead, it changes the power dynamics among interest groups in a way that should neither be ignored nor overstated.

### **Part I: A Theory of Change and Avoidance**

This Article argues that the design of anti-regulatory code is best analyzed as one of many mechanisms that interest groups might use to influence the effects of law. Implicit in this argument are a set of assumptions and arguments that the first part aims to clarify.

#### **A. Studying the Regulated**

##### *On the Limits of General Theories of Regulation*

John Austin, lecturing on jurisprudence in the early 1800s, described the essence of legal study as the effort to separate legal effects from morals, religious scruples, and other distractions.<sup>17</sup> Today's positive legal scholars disobey this admonition to the fullest extent possible. They have pushed the scope of the positive study of regulation to its maximum extent, with general theories of regulation that include anything that can be plausibly said to "regulate."<sup>18</sup> Theorists routinely study the regulatory effects of law, group rules, social norms, and even the regulatory potential of code.<sup>19</sup> This

---

<sup>17</sup> See John Austin, *The Province of Jurisprudence Determined* 26 (1832).

<sup>18</sup> See, e.g., Robert Ellickson, *Order Without Law* 126-32 (1991) (describing five different sources of regulation); Lessig, *supra* note 4, at 86-90 (1999) (describing four modalities of regulation: law, markets, norms, and architecture (code)). The antecedents for such general theories are in the sociology literature, see The antecedents are in related sociological efforts, see, e.g., Donald Black, *Preface*, in *1 Toward a General Theory of Social Control* xi (Donald Black, ed. 1984).

<sup>19</sup> See *id.*

scholarship reflects an effort to understand all the “forces” of regulation that might be acting on an individual, reasoning that understanding the study of law alone gives an incomplete picture. Robert Ellickson, in *Order without Law*, even gave this pejorative label: “legal centralism.”<sup>20</sup>

But there’s something lopsided to this effort. Current scholarship has paid great attention to the options available to regulators. But how does it account for the reactions of the regulated? The spirit of positive scholarship is to leave no stone unturned in the assessment of regulatory effect. Fidelity to that approach surely necessitates understanding not only what regulates, but also a full account of how the regulated might undermine or compromise a regulatory scheme. If the goal of positive scholarship is to understand the net effect of the regulatory forces acting on a body, the model is necessarily incomplete without a full accounting of the reaction to those forces. A regulator should be able to anticipate that, faced with a disagreeable law, that groups and individuals will react. But what form will such reactions take? And how effective will they be?

Today, these questions are answered in ways by different bodies of scholarship. In general, one answer comes from the compliance literature: that groups will *avoid* laws they find burdensome. Another answer comes from writings in political choice: groups will act to *change* disagreeable laws. This Part proposes to reconcile and unite these divergent account of the behavior of the regulated by analyzing the choice between *avoidance* and *change*. The goal is to understand when and why groups might choose one or the other, to derive a more general theory of how groups react to burdensome laws, and what consequences attend such decisions.

The first section describes the basic assumptions and how the mechanisms of avoidance and change are studied in current scholarship. The second section describes a simple model for describing investments in mechanisms to influence the effects of law. The third section explores consequences of the change / avoidance dichotomy.

## **B. When Groups Get Sick of Complying**

What choices face an individual or group who decide to quit complying with the law and invest in some mechanism to change its effects? This section outlines the fundamental choice between efforts to *change* and efforts to *avoid* laws with which they disagree.

---

<sup>20</sup> Ellickson, *supra* note 18, at 4, 137-147. Oliver Williamson coined the phrase, see *Credible Commitments: Using Hostages to Support Exchange*, 73 *Am. Econ. Rev.* 519, 520 (1983) while Ellickson popularized and expanded on its weaknesses.

First, a few assumptions should be made clear. Laws and other regulations prevent groups from doing what they would otherwise want to. As Tom Tyler puts it, “Laws are passed and enforced to mandate behavior that people would prefer to avoid .... It is a basic tenet of political theory that any society ... fails to provide its citizens with some thing they want and feel they deserve.”<sup>21</sup> A related assumption is that the initial content of laws are exogenous, the result of an unspecified political process.<sup>22</sup> As a result, groups often face laws the content of which they disagree and would prefer to not follow, either in individual cases or as a general matter. And to begin with, compliance is driven by expected costs (punishments), whose source is legal (other sources are possible, but omitted for the present).<sup>23</sup> Finally, a mechanism of legal influence is anything that, for a given price, buys a decrease in the expected punishment from a given law. For example, a \$40 radar detector that eliminates any chance of being caught speeding is such a mechanism.

#### *Avoidance Mechanisms*

When and why do groups obey the law? Basic economic models of compliance give a very simple answer: that laws are followed when the expected costs of legal punishment exceed the expected benefits of the banned behavior.<sup>24</sup> The result is commendably simple, but only because it does not give an accurate account of when law is obeyed. As theorists point out, it neglects two important contributing factors. The first is extra-legal forces, such as social norms, that might contribute to compliance. The second is investments in mechanisms of avoidance, or efforts that would lower the expected costs of the law, that might lead to greater non-compliance.

Efforts to broaden the basic model have focused on the first point, focusing on the role that social norms and other factors play in creating

---

<sup>21</sup> Tom Tyler, *Why People Obey the Law* 19-20 (1990).

<sup>22</sup> The assumption that the content of laws is exogenous becomes difficult to maintain when we consider changing laws as a mechanism of response. In a subsequent section, I consider what happens when the assumption that laws are exogenous is relaxed. See *infra*, text accompanying notes 70 to 77.

<sup>23</sup> Cf. Leo Katz, *Ill-Gotten Gains: Evasion, Blackmail, Fraud And Kindred Puzzles Of The Law* 17-30 (1996) (Describing avoision of moral and ethical rules as comparable to avoision of law).

<sup>24</sup> Albeit with much built into each side of the equation. See Richard Posner, *Economic Analysis of Law* § 7.2, at 242. (“The model can be very simple: A person commits a crime because the expected benefits of the crime to him exceed the expected costs.”).



compliance. Both theory and some empirical studies suggest that the threat of legal punishments alone cannot and does not fully explain why people obey or do not obey the law.<sup>25</sup> Supplemental explanations tend to rely either on normative theories, or more advanced models of self-interested behavior. Some, like Tom Tyler, argue that normative considerations are central to understanding the public's decision to comply or not.<sup>26</sup> Others, like Eric Posner, model extra-legal compliance as self-interested signaling,<sup>27</sup> while still others have modeled extra-legal compliance as a part self-interested models of group interaction following game-theoretic models.<sup>28</sup>

This section, however, is focused on a different criticism of the basic economic model of compliance: that it fails to take into account investments in efforts to avoid the law. As much as the regulative effect of social norms may create more compliance than the basic model predicts, investments in efforts to decrease or eliminate punishments may result in less compliance than predicted. In this area, Gary Becker and George Stigler first argued that investments in avoidance should be considerations of compliance, in their

---

<sup>25</sup> See, e.g., Robert Ellickson, *Order Without Law* 137-147 (1991) (arguing that law's punishments only explain some of the social order we see); Paul G. Mahoney & Chris William Sanchirico, *Norms, Repeated Games, and the Role of Law* (2002) (unpublished manuscript at 41-48) available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=311879](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=311879) (suggesting that state punishment of deviants supports social orders otherwise maintained by group sanctions); Eric Posner, *Law And Social Norms: The Case Of Tax Compliance*, 86 *Va. L. Rev.* 1781, 1782 (2000) (observing that state punishment cannot explain tax compliance); Tom Tyler, *supra* note 21, at 22-27 ("the legal system cannot function if it can influence people only by manipulating rewards and costs."). With mixed answers, some of the empirical studies of the relationship between legal threats and compliance include Isaac Ehrlich, *Crime, Punishment, and the Market for Offenses* (surveying empirical work in this area); Raymond Paternoster, *The Deterrent Effect of Perceived Certainty and Severity of Punishment: A Review of the Evidence and Issues*, 4 *Just. Q.* 173 (1987) (suggesting weak correlation between perceived certainty of detection and drug use); Daniel S. Nagin & Raymond Paternoster, *The Preventive Effects of the Perceived Risk of Arrest: Testing and Expanded Conception of Deterrence*, 29 *Criminology* 561, 580-81 (1991) (arguing that certainty of punishment plays a clear but minor role in determining compliance).

<sup>26</sup> See generally, Tyler, *supra* note 21; see also, E. Allan Lind & Tom R. Tyler, *The Social Psychology of Procedural Justice* 230-231 (1988) (developing group value model to explain compliance).

<sup>27</sup> Eric A. Posner, *Law and Social Norms* 88-111 (2000). Posner points out that the normative and self-interested models of compliance can be unified by noting that effective signaling depends on laws being considered legitimate. See *id.* at 111.

<sup>28</sup> See, e.g., Ellickson, *supra* n. 18, at 137-147; generally, Mahoney & Sanchiro, *supra*, note 18.

classic *Law Enforcement, Malfeasance and Compensation of Enforcers*.<sup>29</sup> They added investments in bribery or intimidation to a model of criminal behavior, pointing out that if a person had already violated the law, she would be willing to invest up to the costs of the sanction to avoid punishment.<sup>30</sup> This insight suggests a very basic point: that compliance is not simply a function of punishments, but can be rather a function of the cost of mechanisms to avoid punishment.<sup>31</sup>

But it is the compliance literature surrounding particular statutory regimes that gives more particularized insight into how groups avoid laws. This is a particular focus of writings on tax compliance,<sup>32</sup> and is also the subject of study in labor law,<sup>33</sup> criminal law,<sup>34</sup> environmental law,<sup>35</sup> and international

---

<sup>29</sup> See Gary Becker & George Stigler, *Law Enforcement, Malfeasance and Compensation of Enforcers*, 3 *J. Legal Studies* 1 (1974).

<sup>30</sup> *Id.* at 2-6. The observation was a short stop enroute to their proposal for private enforcement of criminal law, and the debate over their paper has focused on the merits of private and public law enforcement. See, e.g., See Mark A. Cohen & Paul H. Rubin, *Private Enforcement of Public Policy*, 3 *Yale J. Reg.* 167 (1985) (arguing for shifting responsibility for implementing and enforcing public policy to private enforcement agents); William M. Landes & Richard A. Posner, *The Private Enforcement of Law*, 4 *J. Legal Stud.* 1 (1975) (responding to Becker & Stigler's proposal to privatize criminal law enforcement).

<sup>31</sup> This insight is described in greater depth in text accompanying notes 64 to 68, *infra*.

<sup>32</sup> See, e.g., Posner, *supra* note 58, at 1782 (proposing a signaling model rather than the standard state sanctioning model to explain tax compliance); Michael Graetz et al., *The Tax Compliance Game: Toward an Interactive Theory of Law Enforcement*, 2 *J. L. & Econ. & Org.* 1 (1986) (modeling tax compliance as game); Marsha Blumenthal et al., *Do Normative Appeals Affect Tax Compliance? Evidence from a Controlled Experiment in Minnesota*, 54 *Nat'l Tax J.* 125 (2001) (concluding from a tax compliance study that normatively appealing to taxpayer's conscience via a letter had an insignificant overall impact on tax compliance); David A. Weisbach, *Formalism in the Tax Law*, 66 *U. Chi. L. Rev.* 860, 884 (1999) (arguing that anti-abuse standards would be more efficient than rules at curbing tax avoidance).

<sup>33</sup> See Ronald Turner, *Reactions Of The Regulated: A Federal Labor Law Example*, 17 *Lab. Law.* 479 (2002) (detailing ways in which groups practice "avosion" of labor laws).

<sup>34</sup> See, e.g., Neal Kumar Katyal, *Deterrence's Difficulty*, 95 *Mich. L. Rev.* 2385, 2414-15 (1997) (noting that a deterrence model in criminal law should focus on the role of substitute products and complements to banned products and behavior.).

<sup>35</sup> See, e.g., Keith N. Hylton, *When Should We Prefer Tort Law To Environmental Regulation?*, 41 *Washburn L.J.* 515 (2002) (comparing the benefits of using tort law as a system of privately-enforced environmental protection to traditional public statute-based regulatory schemes).

law.<sup>36</sup> From these areas comes a recognition that there are two fundamentally different ways of avoiding a law. The first can be termed *evasion*: or simply an investment in decreasing the odds of being punished for violating a law. Wearing a mask to rob a bank; buying a radar detector, hiring expensive defense lawyers, and bribing police officers are all examples.<sup>37</sup> Each, for a certain price, decreases the odds of being punished for breaking the law.

Another way of avoiding law, however, is *avoidance*, or efforts to exploit loopholes: differences between a law's goals and its self-defined limits. As Ronald Turner describes it, such are "efforts to change legal mandates or the avoidance of laws in ways that evade the law's intent or purpose but do not actually constitute unlawful behavior."<sup>38</sup> Consider the example of the pornographer who, worried about running afoul of decency laws, puts his photos in a book along with incisive essays on "sex in marriage." Or the taxpayer whom, blocked by deducting a transfer of money to her son, devises a complicated loan scheme to achieve the same effect. Leo Katz's book on avoidance is full of such examples, from law and other aspects of life.<sup>39</sup> A similar effect can be seen in Neal Katyal's study of the role of substitute products in criminal deterrence.<sup>40</sup> If, for example, the goal of the drug laws is to prevent addiction and abuse, a person opts to become an alcoholic (legal) instead of a crack addict (illegal), is practicing avoidance.

From these writings we are left with the following picture. Groups, to minimize the burdens of laws, will sometimes invest in avoidance. If the price is right (more on this later),<sup>41</sup> they will invest in mechanism to lower or eliminate the probability of being punished for disregarding a law.

Yet, even at its fullest extent, the study of compliance still delivers a limited picture of how individuals or groups might try to defeat a regulatory scheme. The focus is groups may either decrease the probability of detection (as in Becker's example of a bribe), or to adapt conduct into other forms with

---

<sup>36</sup> Compliance in international law is studied in the absence of a centralized enforcement system, creating concerns more akin to the study of compliance with social norms. See, e.g., Abram Chayes and Antonia Chayes, *The New Sovereignty: Compliance with International Regulatory Agreements* (1995) (studying compliance with treaties); Jack Goldsmith & Eric Posner, *A Theory of Customary International Law*, 66 U. Chi. L. Rev. 1113 (1999) (studying compliance with customary international law).

<sup>37</sup> Some of these are ex poste examples, others are ex ante. For present purposes they are considered together.

<sup>38</sup> See Turner, supra note 33, at 479.

<sup>39</sup> See generally, Leo Katz, *Ill-Gotten Gains: Evasion, Blackmail, Fraud, and Kindred Puzzles of the Law* (1996).

<sup>40</sup> See generally Katyal, supra, note 34.

<sup>41</sup> The effect of prices of such mechanisms is discussed infra, text accompanying notes 64 to 68.

the same effects (as in Katyal's substitution effect, or Katz's avoision). Yet it is also often the case that groups will react to burdensome laws with an effort to *change* the law, either by lobbying for change, or pursuit of a litigation strategy.

### *Change*

It is by now a familiar insight from public choice theory that groups who find a disagreeable may try to change it.<sup>42</sup> Such mechanisms of change, such as lobbying, can be studied as general alternative to avoidance for influencing the effects of law.

In the early 1990s, the dietary supplement industry faced a serious legal threat. Following several well publicized deaths, the FDA had proposed to regulate popular dietary supplements like other drugs, requiring proof of therapeutic value and carefully determined dosages.<sup>43</sup> Their reaction was to invest in an expensive but successful lobbying campaign to change the law. Within a short time Congress had passed legislation limiting the FDA's authority to regulate their product.<sup>44</sup> Today the supplement industry remains virtually unregulated.<sup>45</sup>

The example is hardly unique. Public choice theory accounts for and models such investments in favorable legislative change. In the 1970s, a series of articles written by economists Stigler and Peltzman,<sup>46</sup> followed by McCormick and Tollison's *Politicians, Legislation, and the Economy*,<sup>47</sup> first modeled legislation as wealth transfers that interest groups purchased with money and votes. As Peltzman put the basic premises: "I begin with the

---

<sup>42</sup> A summary of work in this area is Dennis C. Mueller, *Political Choice II* (1989), particularly chapters 13 and 16.

<sup>43</sup> See Regulation of Dietary Supplements, 58 Fed. Reg. 33,690 (proposed June 18, 1993).

<sup>44</sup> See The Dietary Supplement Health and Education Act of 1994, Pub. L. No. 103-417, 108 Stat. 4325, 4326 (1994). This Act amended the Federal Food, Drug and Cosmetic Act ("FDCA") classifying dietary supplements as a new category of food, and thereby preventing the FDA from regulating supplements as drugs or food additives.

<sup>45</sup> See Peter A. Vignuolo, Note, *The Herbal Street Drug Crisis: An Examination of the Dietary Supplement Health And Education Act of 1994*, 21 Seton Hall Legis. J. 200, 220-23 (1997).

<sup>46</sup> See George J. Stigler, *The Theory of Economic Regulation*, 2 Bell J. of Econ. & Man. Sci 3 (1971) (presenting general interest group theory of politics); George J. Stigler, *The Size of Legislatures*, J. Legal Studies 5 (1976); Sam Peltzman, *Toward a More General Theory of Regulation*, 2 J. Law & Econ. 211 (1976).

<sup>47</sup> R.E. McCormick & R.D. Tollison, *Politicians, Legislation and the Economy* (1981).

presumption that what is basically at stake in regulatory processes is a transfer of wealth ... beneficiaries [of wealth transfers] pay with both votes and dollars."<sup>48</sup> Or as Professors Richard Posner and William Landes described the legislative process, laws are sold for "campaign contributions, votes, implicit promises of future favors, and sometimes outright bribes"<sup>49</sup>

The basic model sees legislative change as a commodity available for purchase. Since that time, the literature studying the specific mechanics of interest-groups and law-making has become quite sophisticated. Fred McChesney, for example, proposes that law-makers are more extortionists than bribees.<sup>50</sup> He suggests that lobbying is primarily defensive: Congress threatens legislation that groups pay to avoid: much of the political process can be better described as rent-extraction instead of rent-creation.<sup>51</sup> A series of papers in the economics literature, meanwhile, tries to improve on the simple bribery model of with informational concerns, asserting that lobbying works through the selective presentation of information.<sup>52</sup> But despite these refinements, lobbying is still studied in an essentially mechanistic manner. It remains a tool that delivers or prevents legal change for a price.

The process of achieving legal change through litigation has also, though less often, studied on the basis of an investment or quid-pro-quo model. In Professor Landes & Posner's first analysis of the independent judiciary, litigation served as a means of extending the value of the legislative bargains made between interest groups and the legislators.<sup>53</sup> Jeremy Rabkin, in a 1989 work, broadly argued that interest groups through their litigation strategies, determined or radically influence the regulatory agendas of agencies.<sup>54</sup>

---

<sup>48</sup> Peltzman, *supra* note 46, at 213-214.

<sup>49</sup> William Landes & Richard Posner, *The Independent Judiciary in an Interest Group Perspective*, 18 *J.L. & Econ.* 875, 877 (1975)

<sup>50</sup> See Fred S. McChesney, *Rent Extraction and Rent Creation in the Economic Theory of Regulation*, 16 *J. Legal Studies* 101 (1987); see also Fred S. McChesney, *Money for Nothing* (1997) (developing and broadening the rent extraction model).

<sup>51</sup> McChesney, *supra* note 50, at 109-112.

<sup>52</sup> Austen-Smith, David, and John R. Wright, *Competitive Lobbying for Legislators' Votes*, 9 *Social Choice and Welfare* 229-257 (1992); Johan Lagerlof, *"Lobbying, Information and Private and Social Welfare"*, 13 *European Journal of Political Economy* 615-637 (1997); Susanne Lohmann, *Information, Access, and Contributions: A Signaling Model of Lobbying*, 85 *Public Choice* 267-284 (1995).

<sup>53</sup> See Landes & Posner, *supra* note 49; Richard Posner, *Economic Analysis of Law* §§20.1-20.2 (4th ed. 1992).

<sup>54</sup> Jeremy Radkin, *Judicial Compulsions: How Public Law Distorts Public Policy* (1989).

And Einer Elhauge in 1991 essay argued that the litigation process was, equally is not more susceptible to interest group influence.<sup>55</sup> He argued that “the same interest groups that have an organizational advantage in collecting resources to influence legislators and agencies generally also have an organizational advantage in collecting resources to influence the courts.” Therefore, “[I]ncreasing the lawmaking power of the courts may only exacerbate the influence of interest groups.” Whether Elhauge’s specific conclusion is right or wrong, he demonstrates that litigation campaigns can also be modeled as investments in legal change.

From this we can see that strategies lobbying or litigation can be viewed, aside from their other roles, as an alternative mechanism for influencing the costs of law. Some, clearly, may think the comparison here developed strange or misguided. The description is thin; there is, first of all, a side to changing laws that cannot be simply described as reactions to undesirable laws. And on normative grounds, lobbying for change, while controversial, is surely an unavoidable part of a pluralist system of government. Avoiding enforcement, on the other hand, apart perhaps in instances of civil disobedience, is almost never said to be a good thing.<sup>56</sup> It is also hard to describe avoidance as forming part of the legal system in the same sense. Are the processes of law-making and law-enforcement better left as separate fields.

I maintain that it is nonetheless useful and instructive to consider change and avoidance as distinct options for interest groups efforts to respond to laws. A parallel can be drawn to Albert Hirschman’s famous work of institutional feedback, *Voice, Exit and Loyalty*. Hirschman emphasized that members of declining institutions faced a fundamental choice between “voice” and “exit” as forms of feedback.<sup>57</sup> This part suggests that focusing on the choice between *avoidance* and *change* for groups faced with burdensome laws will yield similar dividends. As with voice and exit, we want to know the conditions under which each option will prevail, and their comparative efficiency. And the comparison leads to further normative questions. If *change* mechanisms are a preferred mechanism of engagement, how can law-makers encourage groups to invest in change? Finally, if the tools of avoidance grow in sophistication, as the example of code design here featured suggests, it makes sense to understand what the consequences will be.

---

<sup>55</sup> See Einer R. Elhauge, Does Interest Group Theory Justify More Intrusive Judicial Review?, 101 Yale L.J. 31, 67-68 (1991);

<sup>56</sup> But see Katz, supra note 39 (defending the ethics of avoidance in certain circumstances.)

<sup>57</sup> See Albert O. Hirschman, Exit, Voice and Loyalty 3-5 (1970).

## B. Group Dynamics, Collective Action, and the Change / Evasion Dichotomy

The distinction between a group's choice of a change or avoidance strategy is, I suggest, fundamental to understanding how groups deal with laws they do not like. This section links that choice to questions of group dynamics and problems of collective action.

In 1965, Mancur Olson made a contribution to the study of interest group behavior of lasting relevance.<sup>58</sup> Using the logic of collective action, he outlined a central distinction between groups affected by regulation. The distinction lay between, on the one hand, groups capable of effective political action, and the "forgotten groups," who, he argued "suffer in silence."<sup>59</sup> The dividing line lay in the ability to overcome collective action problems. Olson asserted that effective political action would generally represent a problem of collective action, leaving small groups and those organized for some other purpose (like unions) as effective political actors, while the large and disorganized were essentially victims to the legislative process.<sup>60</sup> His model predicted that lobbies representing business, labor, agriculture and professionals would enjoy a perpetual advantage, leaving consumers and other latent groups forgotten, and even oppressed.<sup>61</sup>

The change / avoidance dichotomy suggests something different. Forgotten groups don't necessarily suffer in silence: instead, they *avoid* laws they disagree with if it is convenient to do so. In the terms used here, the groups Olson identified as incapable of collective action will generally lack the capacity to invest in change mechanisms. But that doesn't necessarily make them inert under burdensome laws. Rather, their recourse is limited to investing in avoidance mechanisms to decrease the costs of laws. That is to say, Olson's dichotomy between groups can be better understood as a indication of who can take advantage of *change* mechanisms. The logic of

---

<sup>58</sup> See Mancur Olson, *The Logic of Collective Action* (1965). The logic of collective action and problems of free-riding now underlie most present day study of lobbying and interest group behavior. See, e.g., McCormick & Tollison, *supra* note 47, at 17-18 (discussing organizing costs); Daniel A. Farber & Philip P. Frickey, *Law and Public Choice: A Critical Introduction* 17-21 (1991); Glynn S. Lunney, Jr., *A Critical Reexamination of the Takings Jurisprudence*, 90 *Mich. L. Rev.* 1892, 1949-52 (1992) (summarizing the lobbying advantages available to a small interest group);

<sup>59</sup> Olson, *supra* note 58, at 165.

<sup>60</sup> *Id.* at 53-57, 132-134, 165-167.

<sup>61</sup> *Id.* at 133-167.

collective action dictates how groups deal with laws they don't like. It isn't that forgotten groups have no options for influencing the effects of law; it is that their options are more limited.

All this follows because *change* presents a collective action problem, while *avoidance* does not. Changes in laws display the classic attributes of public goods. The repeal of the prohibition on alcohol in the 18th Amendment,<sup>62</sup> for example, benefited all drinkers, not just those who contributed to the effort.<sup>63</sup> Nor was there any possibility that the repeal would be consumed or dissipating by over-use. As a result, economic theory predicts a free-riding or collective action problem: the beneficiaries of the change will wait for others to invest in change, and free-ride on those efforts. But none of this is true of avoidance mechanisms. When a thief wears a mask to rob a bank, he is the sole and directly beneficiary of his investment. When a firm invests in a complicated tax-avoiding scheme, their competitors do not also benefit. In other words, the investments in avoidance mechanisms create private goods: excludable from others, and rivalrous in consumption. As a result, members of large and disorganized groups may invest in mechanisms of avoidance without any need to coordinate with their peers. That fact drives the choice between avoidance and change mechanisms.

At this point, we may lay out the relevant distinctions in effect and incentives between mechanisms of avoidance and change:

	<u>Change</u>	<u>Avoidance</u>
Examples	Lobbying	Tax Shelter Bribery
Target	Prohibition	Probability of Detection
Incentives	Collective Action Problem	Benefits captured individually
Scope	General	Specific; vulnerable laws

<sup>62</sup> See U.S. Const. Amend. XXI § 1.

<sup>63</sup> The repeal also cannot be "used up" by overconsumption. Legal change is an example of what economists call a public or collective good: it is both non-rival and non-excludable. See Olson, *supra* n. 58, at 14 n. 21 (defining public good).



#### D. Deciding to Quit

Groups don't spend all their time avoiding laws or trying to change them: most people comply with most laws most of the time. So when do individuals or groups decide to quit and invest in some way to way to avoid or change law? The basic deterrence model discussed above suggests that this happens when the costs of compliance exceed the expected costs of punishment. Theorists have supplemented that model with compliance from social norms and other sources. I propose that we can further derive a better answer by introducing the option of investing in mechanisms to decrease legal<sup>64</sup> or other costs. The following will show that compliance may sometimes less on punishment than on the cost of mechanisms of change and avoidance punishment. It will also demonstrate the effect of a group's ability act collectively, pooling resources to invest in legal change.

First, the basic case, where groups obey the law when expected costs exceed expected benefits, and there are no mechanisms to influence the law. If a speed law mandates a 55mph limit, the expected benefit of ignoring the law and driving 80mph might be \$50, while the expected cost will be the price of the speeding ticket multiplied by the chance of getting caught (say, 20% times \$500 = \$100.) With these numbers, the driver will not speed—the result is compliance, and the law is a “success.”

##### Compliance With No Investments in Response

Assume:

- (1) Speed limit = 55mph
- (2) Benefit of driving 80 mph = \$50
- (3) Expected Costs = (Sanction)(Probability of Detection) = 500 x 0.2 = \$100

Result: Driver complies with law, because expected costs > expected benefits

We can now add the option of investing in a mechanism that influences the expected costs of the law. As discussed above, Becker & Stigler's original example was the bribe: for a certain fee, a bribe reduces the expected costs of a law to zero (by eliminating any chance of detection).<sup>65</sup> But there are a wide variety of mechanisms beyond bribes that will accomplish the

<sup>64</sup> A caveat. At this stage, the model that follows is admittedly legally-centrist. For simplicity's sake, it does not include the compliance produced by norms or other modalities of regulation.

<sup>65</sup> Becker & Stigler, *supra* note 6, at 5-6.

same effect. For our driver, we might consider one example of *avoidance* and one of *change*: investing in a radar detector, or lobbying to repeal the speeding law, respectively.

Individuals and groups will invest in a mechanism of legal influence when it becomes cheaper to do so than to simply comply with the law. That is to say, investments in such mechanisms come at the point where the forgone benefits exceed the price of the response strategy, plus the expected costs of non-compliance (as reduced through the mechanism).

This verbalization can be described with a very simple equation. Groups who have the option of purchasing mechanisms of legal influence, will comply when:

$$(4) \quad \text{Expected Benefits} > (\text{Expected Costs} - \text{Mechanism Effect}) + \text{Cost of Mechanism}$$

This can be applied to two examples: radar detectors and lobbying. First, consider a \$40 radar detector that eliminates any chance of being caught speeding. For the driver discussed above, this is a worthwhile investment. For the price of the radar detector (\$40), he gets to drive at 80mph (benefit \$50) and is therefore \$10 ahead. The driver is pleased, but the regulator is not: the law that was once a “success” is now a “failure.”<sup>66</sup>

#### Compliance Given a Perfect \$40 Radar Detector

Assume:

- (5) Radar detector makes probability of detection = 0%
- (6) Expected benefit of speeding = \$50
- (7) Expected cost of radar detector = \$40
- (8) Expected cost of legal punishment =  $500 \times 0 = 0$

$$50 > 0 + 40$$

Result: Driver disregards law

What this shows that if the mechanism of legal influence is effective, like our radar detector (reducing expected costs of legal sanctions to zero) the cost of the strategy replaces the expected costs of law in the basic equation of compliance. The only relevant inputs are the forgone benefits and the cost of

<sup>66</sup> Notice that for simplicity’s sake, this hypothetical has neglected the government’s response: government can, as many states do, ban the radar detector (but more on this later).

the response strategy. Therefore, given effective mechanisms, the equation can be simplified as follows:

Compliance when:

(9) Expected Benefit > Cost of Mechanism

In other words, in a world where avoidance or change is effective, compliance has little to do with punishment; but is instead a direct function of how much it costs to buy a way out.

There are several implications of this approach. If the speed limit were 100mph, and hence not much of a burden, few would buy the perfect \$40 radar detector. Conversely if the speed limit were lowered to 10mph, and an onerous burden, everyone will want one, even if it costs \$500. Finally, notice that if the perfect radar detector suddenly falls in price to \$1, it may suddenly become a worthwhile investment even for the nearly costless 100mph speed limit.<sup>67</sup>

The second example is a lobbying campaign. Say it would cost \$100,000 to organize a campaign to repeal the speeding laws. For the individual driver, the lobbying campaign is not a worthwhile purchase. The benefit of driving at 80mph is only \$50. The cost of the campaign would leave the driver \$99,550 in the red, unless he were somehow able to charge his fellow drivers for his successful repeal, an unlikely prospect.

<p><b>Compliance Given a \$100,000 Lobbying Campaign</b> Assume:</p> <p>(10) Repeal makes expected costs = \$0  (11) Expected benefit of speeding = \$50  (12) Expected cost of campaign = \$100,000</p> <p>50 &lt; 100,000</p> <p>Result: Driver complies with law.</p>
--

67

response strategy for any investment to happen at all. This is a consequence of perspective—the assumption is that the individual is complying with the law, and deciding whether to invest in some way to make it worthwhile not to. In contrast, Stigler and Becker’s original model posited a criminal already in violation of the law, and suggested the violator would “be willing to bribe as much as [the fine] to ignore the evidence.” Stigler & Becker, supra note 29, at 5. While the behavior of violators is of interest, it seems more generally interesting to understand what individuals already regulated by the law will do, instead of assuming that they will break it.

But would it make sense for the affected group (all drivers) to invest in a campaign to repeal the speeding laws? Assume that there are 100,000 drivers in the lawmaking jurisdiction (state). If the drivers organize themselves to divide the costs of the repeal campaign, it amounts to \$1 each, and is clearly a good deal. Stated otherwise, the cost of compliance for the group is \$50 times 100,000 drivers, or \$5 million. The lobbying campaign is, therefore, a bargain.

**Compliance Given a \$100,000 Lobbying Campaign (2)**

Assume:

(12) Repeal makes expected costs = \$0

(13) Group expected benefit of speeding = \$5 million

(11) Expected cost of campaign = \$100,000

\$5 million > 100,000

Result: Group repeals speeding laws.

If these numbers are even close to realistic, then why are there any speeding laws or any other laws that large groups find disagreeable? The answer, as already seen and as basic political choice theory teaches, is that groups like drivers aren't organized, and have no effective mechanism to split the costs of a campaign to change the law.<sup>68</sup> Hence, as this section suggested, groups incapable of collective action tend toward *avoidance* mechanisms, while the organized invest in mechanisms of *change*.

\* \* \*

Finally, a more formal way of described difference between avoidance and change mechanisms is by reference to the classic model of expected regulatory cost. Gary Becker modeled the expected cost of

---

<sup>68</sup> See discussion of group dynamics, *supra* text accompanying notes 58 to 63.

regulation as a function of the liability or sanction imposed and the probability of being caught.<sup>69</sup>

$$\text{Regulatory Cost} = (\text{Probability}) (\text{Sanction})$$

Based on this model, the dichotomy between change and avoidance reflects a difference in which input is targeted: either (1) the punishment, or (2) the probability of detection, respectively. Avoidance mechanisms can be described as anything that for a price will decrease the probability of being sanctioned for a given activity. Wearing a mask to rob a bank; buying a radar detector, hiring expensive defense lawyers, and bribing police officers are all examples. Each, for a certain price, decreases the odds of being punished for breaking the law. On the other hand, change mechanisms can be described as efforts to decrease or eliminating the punishment attending certain forms of behavior. The example of the repeal of prohibition or limiting the FDA's authority over dietary supplements are both examples.

#### **D. A Hierarchy of Mechanisms**

This section has discussed the idea that groups choose between change and avoidance mechanisms to influence the law. But are the two mechanisms of equal or different efficacy? Stated another way, is there a way to know whether some laws may be more or less vulnerable to different mechanisms of influence?

The principle differences between the mechanisms of change and avoidance is that the former are general while the latter depend on specific vulnerabilities or loopholes in the law. For avoidance (either avoision or evasion) to work, either the logical structure of the law or its enforcement structure need contain an exploitable weaknesses. Conversely, the greatest potential of the mechanisms of legal change discussed is fundamentally an institutional question. How sympathetic is the agency or legislature to the group's concerns? For this reason, change mechanisms can be regarded as greater efficacy for interest groups, provided the groups has the capability to use such mechanisms.

Consider just one example of how a legal regime can be more or less vulnerable to evasion. This is the degree of dependence of *primary* as opposed to *supplemental* enforcement. That is to say, laws whose enforcement depends on mass enforcement can be the target of effectively

---

<sup>69</sup> See Gary Becker, Crime and Punishment: An Economic Approach, 76 J. Pol. Econ. 169 (1968).

targeted by an evasion mechanism. On the other hand, effective supplemental mechanisms: gatekeeper regimes, systems of social norms, and otherwise, render a legal regime less vulnerable.

A mechanism of evasion may target a law dependent solely on primary enforcement, or else itself represent some means of undermining supplemental enforcement schemes. But this theoretical limit serves as a major constraint as compared with mechanisms of legal control.

### **E. Avoidance, Change, and Regulatory Competition**

Up to this point, the analysis has focused on the first generation of reactions: those of an interest group to a disagreeable law. This section outlines how “reactions to the reaction” can lead to a regulatory competition between two opposed groups, each investing in efforts to influence the law in its favor. For this analysis, the framework of a rent-seeking competitions is a useful descriptive, if not necessarily normative, guide.

Until this point, laws have been modeled simply as exogenously imposed costs on regulated groups. A more realistic model recognizes that for every *regulated* group there exists also a *beneficiary* groups.<sup>70</sup> If a law bans noisy sound trucks, the advertisers are the regulated, while town residents are the beneficiaries.<sup>71</sup> Successful efforts to avoid or change the law may, therefore, inspire the beneficiary group to invest in its own mechanism of legal influence in an effort to restore the lost benefit. This, in turn may inspire the regulated group to reinvest in mechanisms of influence, leading to a full-fledged cycle of regulatory competition. The cycle continues as long as each group values sufficiently the prize of a law tailored in their favor.

Just as group identity and dynamics influenced the actions of the regulated group, we should expect the same for the beneficiary group. That is to say, the second generation reaction of the beneficiary group will determine the strength and nature of the reaction to the reaction. An organized, politically effective beneficiary group faced with evasion may turn to Congress with a request to “restore the balance.” On the other hand, diffuse beneficiaries may do little to react effectively.

Consider a contrast in this respect. The P2P story features a subset of music consumers trying to avoid copyright laws, in ferocious competition with the music industry. Faced with a threat to their copyright rents, the

---

<sup>70</sup> Cf. R.E. McCormick & R.D. Tollison, *Politicians, Legislation and the Economy* (1981) (modeling groups in competition for legislative wealth transfers).

<sup>71</sup> See *Kovacs v. Cooper*, 336 U.S. 77 (1949) (sound truck case).

industry reacted with litigation, lobbying and even technological countermeasures, as detailed in Part III. In contrast, avoidance of state taxation through online and mail-order catalogues is now a regular phenomenon. Yet the diffuse beneficiaries of state taxation have done little to resist the eroding collection of state value-added taxes.<sup>72</sup> Unsurprisingly, the organization of the beneficiaries matters as much as for the regulated.

\* \* \*

The notions of regulatory competitions are a favorite subject of the rent-seeking literature, and it is tempting to cast matters in such terms. In Anne Krueger's original description of rent-seeking, for example, she suggested that laws create rents, and that people will compete for them in various way: "[s]ometimes, such competition is perfectly legal. In other instances, rent seeking takes other forms, such as bribery, corruption, smuggling, and black markets."<sup>73</sup> Arguably, any group interested changing a law to minimize its regulatory costs is engaged in a form of rent-seeking. Every reaction of a group to a legal regime can be cast as yet another aspect of the rent-seeking society. The battle between P2P programmers and the recording industry described in Part III can be described as simply a gigantic dissipation of rents created by the monopolistic copyright system.

It is helpful to understand that groups reacting to law are acting in a self-interested fashion, and it is also helpful to see that this may lead to a competition to influence the law's effects. But for several reasons I am hesitant to cast the questions studied in this part within the normative framework of rent-seeking. Rent seeking is a useful tool when it suggests that certain models of regulation will encourage wasteful behavior and should therefore be avoided. In other words, the study of rent-seeking is the study of waste management. But the goals of this Part are different. They are to develop a positive model of the choices that face groups under burdensome regulation. Determining whether the dissipating is "worth" any particular legal regime, is simply beyond the scope of this Part.

In addition, rent-seeking interests is mechanisms is different. What makes a tool interesting to the rent-seeking literature is potential for generating waste and the existence or lack of any socially valuable byproduct. Hence, what is

---

<sup>72</sup> On the contrary, Congress passed the Internet Tax Freedom Act, P.L. 105-277, restricting the power of states to tax internet-based commerce.

<sup>73</sup> Anne Krueger, *The Political Economy of the Rent-Seeking Society*, 64 *Am. Econ. Rev.* 291, 291 (1974) (Laws "give rise to rents of a variety of forms, and people often compete for the rents. Sometimes, such competition is perfectly legal. In other instances, rent seeking takes other forms, such as bribery, corruption, smuggling, and black markets.").

studied for its rent-dissipating effects can range from research and development (when rent dissipation in pursuit of patent follow-ons)<sup>74</sup> to follow-on creation in copyright,<sup>75</sup> to efforts to monopolize.<sup>76</sup> Yet it is critically difficult to evaluate whether alternative mechanisms of undermining legal system have less or more valuable byproducts.<sup>77</sup> Is investing in a tax shelter more or less socially wasteful than lobbying? Such questions seem nearly impossible to answer. So what this Part is interested in about the mechanisms employed by interest groups is not their relative tendency to waste resources, but their relative cost and relationship to group dynamics.

\* \* \*

This concludes the basic theory of mechanisms that underlies the claims in the rest of the paper. The next Part details degree of fit between copyright's structural enforcement weaknesses, and the design of peer networks designs for exploiting these weaknesses.

## **Part II: Exploiting the Weaknesses of the Copyright System**

On December 8, 1999, a group of eighteen record companies announced that they had sued a small startup company for copyright infringement.<sup>78</sup> The claim demanded more than \$100 million in damages,<sup>79</sup> yet the company was virtually unknown. In the mainstream press, the company had previously drawn only a blurb, described by *Fortune* magazine as “a unique online MP3 trading community . . . that enables users to trade songs directly.”<sup>80</sup>

---

<sup>74</sup> See generally, Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 *J.L. & Econ.* 265 (1977) (describing patents as prospects that prevent waste in follow-on development).

<sup>75</sup> See generally, Michael Abramowicz, *Copyright Redundancy*, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=374580](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=374580) (arguing that copyright prevents wasteful redundancy).

<sup>76</sup> See e.g., Richard Posner, *The Social Costs of Monopoly*, 83 *J. Pol. Econ.* 807 (1975)

<sup>77</sup> See *id.*, at 811 (analyzing assumption that expenditures on monopolizing have no socially beneficial byproduct).

<sup>78</sup> See Don Clark, *Recording Industry Group Sues Napster, Alleging Copyright Infringement on Net*, *Wall St. J.*, Dec. 9, 1999, at B18.

<sup>79</sup> *Id.*

<sup>80</sup> *Tune In: MP3 goes mainstream, but Internet music has yet to find its perfect form*, *Fortune*, Dec. 1, 1999, at 268.



This unknown company was Napster. Its product was an application that facilitated the trading of music files. Napster functioned rather like the “bazaar,” alleged by the plaintiffs,<sup>81</sup> but one where all the stuff was good and free. Users logged in, searched a central database of songs that other users had made available, and then took the files they wanted directly from other users’ computers (not from Napster itself)<sup>82</sup> Lawyers for the recording industry accused the little company of operating a “haven” for “music piracy on an unprecedented scale,” and an “online bazaar” for illegal trading.<sup>83</sup> Napster responded that it simply provided a service for users to trade songs.<sup>84</sup>

If not as ruinous as the recording industry suggested it would be,<sup>85</sup> Napster emerged as a powerful force in the distribution of music. At its height, Napster claimed sixty million registered users, and as many twenty-six million active users.<sup>86</sup> By February of 2001, analysts estimated that Napster users were trading nearly three billion songs, or the equivalent of two hundred million CDs, in a single month.<sup>87</sup> The economic effects of Napster on the music industry were, naturally, disputed in litigation.<sup>88</sup> By some

---

<sup>81</sup> Complaint at 2, *A&M Records v. Napster*, 114 F. Supp. 2d 896 (N.D. Cal. 2000) (No. C99-5183-MHP), available at [http://news.findlaw.com/cnn/docs/napster/riaa/napster\\_complaint.pdf](http://news.findlaw.com/cnn/docs/napster/riaa/napster_complaint.pdf).

<sup>82</sup> See Damien Riehl, *Peer-to-Peer Distribution Systems: Will Napster, Gnutella and Freenet Create a Copyright Nirvana or Gehenna?*, *Wm. Mitchell K. Rev.* 1761, 1767 (2001).

<sup>83</sup> Complaint at 2, *A&M Records v. Napster*, 114 F. Supp. 2d 896 (N.D. Cal. 2000) (No. C99-5183-MHP), available at [http://news.findlaw.com/cnn/docs/napster/riaa/napster\\_complaint.pdf](http://news.findlaw.com/cnn/docs/napster/riaa/napster_complaint.pdf).

<sup>84</sup> See Clark, *supra* note 78.

<sup>85</sup> Complaint at 2, *A&M Records v. Napster*, 114 F. Supp. 2d 896 (N.D. Cal. 2000) (No. C99-5183-MHP), available at [http://news.findlaw.com/cnn/docs/napster/riaa/napster\\_complaint.pdf](http://news.findlaw.com/cnn/docs/napster/riaa/napster_complaint.pdf) (alleging that “Napster’s conduct has caused and continues to cause plaintiff’s grave and irreparable harm”).

<sup>86</sup> The estimates of Napster’s use vary. See, e.g., Jon Healey, *Napster CEO Pitching a New Tune to Labels Profile*, *L.A. Times*, November 25, 2001, at C1 (reporting sixty million active users at Napster’s peak); *Napster Use Slumps 65%*, *BBC News*, July 20, 2001, at <http://news.bbc.co.uk/2/hi/business/1449127.stm> (reporting statistics from Jupiter Media stating that Napster had 26.4 million active users in February 2001 before the numbers began to decline).

<sup>87</sup> See Geoff Nicholson, *Will the RIAA pass up Napster’s \$1 billion offer?*, *Wednesday, February 21, 2001*, available at <http://www.hitsquad.com/smm/news/708/>.

<sup>88</sup> See *A&M Records v. Napster*, 114 F. Supp. 2d 896, 909-11 (N.D. Cal. 2000) (summarizing the findings of several studies of Napster’s economic impact). A later study by economist Stan Liebowitz concludes that Napster’s effects were not proven in the Napster litigation, but that peer filesharing should be expected to hurt the music industry in the long term. Stan Liebowitz, *Policing Pirates in the Networked Age*, *Cato*

figures, in 2000 global music sales tumbled nearly half a billion dollars.<sup>89</sup> CD singles (the clearest Napster competitor) declined nearly 40% that year.<sup>90</sup> In contrast, other studies suggested that Napster actually led its users to buy more CDs.<sup>91</sup>

How did any of this happen? How did a simple program have such a powerful effect on the effective levels of compliance with copyright law? Everyone knows the basic story. But students of enforcement and compliance lack an explanation for why the copyright regime proved so vulnerable to code-based attack, while other laws seemingly do not. What is about the enforcement structure of copyright that made it so easy to defeat? And does it have characteristics shared with other legal enforcement systems?

This Part argues that the success of P2P depended on two powerful, and often unrecognized weaknesses of the copyright regime. The first is the law's dependence on a gatekeeper enforcement regime. The second is a severe lack of normative support among the regulated, amounting to a crisis in legitimacy.

This suggests several conclusions about the nature of P2P and code design as mechanisms of avoidance. P2P in particular is likely of legal implication only to the specific weakness of the copyright system. And code design more generally will depend on identifiable weaknesses in legal enforcement.

### A. Copyright and Its Gatekeepers

It is a common intuition that laws have problems with potential mass disobedience, whether at a rock concert or at tax time. The problems stem from the limits and costs of primary enforcement.<sup>92</sup> The costs of raising punishments increases while bringing diminishing returns. Theorists explain these limits as stemming from administrative and third party costs, the limited

---

Policy Analysis No. 438 at 14-15, May 15, 2002, at <http://www.cato.org/pubs/pas/pa438.pdf>.

<sup>89</sup> Patrick Brethour, Music sales tumble 1.3% worldwide, *The Globe and Mail*, Apr. 20, 2001, at B1.

<sup>90</sup> Jeff Leeds, Record Industry Says Napster Hurt Sales, *L.A. Times*, Feb. 24, 2001, at C1.

<sup>91</sup> See *A&M Records*, 114 F. Supp. 2d at 910 (citing several studies but refusing to rely on them); Kim Chipman, Napster More Likely to Help, Not Hurt, Music Sales, *Bloomberg News*, July 21, 2000 (noting that "most attrition [cited by the RIAA] took place before Napster's launch"); Liam Lahey, Angus Reid Study: Napster is improving CD sales, *ComputerWorld Canada*, Sept. 22, 2000, at 1.

<sup>92</sup> See *supra* note 101.

net worth of defendants, the lack of any punishment beyond the death penalty, and even the Constitutional prohibition of cruel and unusual punishments.<sup>93</sup>

Due to the limitations of primary enforcement, many legal regimes charged with mass regulation come to depend on supplemental enforcement measures. A chief example is what Professor Kraakman termed a “gatekeeper” regime.<sup>94</sup> To supplement direct enforcement of a law, the state attaches liability to the provision of specialized goods or services, disrupting misconduct in advance.<sup>95</sup> Doctors, for example, are gatekeepers for prescription drugs. By withholding their provision of drugs to would-be abusers, doctors aid in the enforcement of the laws regulating controlled substances.

Copyright’s long dependence on a gatekeeping regime is under-recognized.<sup>96</sup> The law regulates a large and disparate group: consumers of content, such as music listeners and book readers. The solution to mass disobedience has been what is now described as a gatekeeper regime. That is,

---

<sup>93</sup> These reasons are summarized in Richard Posner, *Economic Analysis of Law*, §7.2, 243-50 (5th ed. 1998); Kraakman, *supra* note 12, at 56-57. See also Neal Kumar Katyal, *Deterrence’s Difficulty*, 95 *Mich. L. Rev.* 2385, 2414-15 (1997) (“But the range of sanction levels may be subject to a maximum sanction constraint — either because there is no room for increased penalty (beyond death) or because such equality in punishment would contravene other, moral, theories of punishment.”).

<sup>94</sup> Kraakman, *supra* note 12 **Error! Bookmark not defined.**, at 53.

<sup>95</sup> In his influential 1986 article, Kraakman demonstrated that gatekeeper liability could be expected to create additional deterrence relative to primary enforcement. See *id.* at 87-93. That article has inspired a gatekeeper literature, primarily focused on gatekeepers in the financial services industries. See, e.g., Stephen Choi, *Market Lessons for Gatekeepers*, 92 *Nw. U. L. Rev.* 916, 918 (1998); Luigi Alberto Franzoni, *Independent Auditors As Fiscal Gatekeepers*, 18 *Int’l Rev. L. & Econ.* 365, 365 (1998); Ronald J. Gilson, *The Devolution of the Legal Profession: A Demand Side Perspective*, 49 *Md. L. Rev.* 869, 883-84 (1990); Frank Partnoy, *Barbarians At The Gatekeepers?: A Proposal For A Modified Strict Liability Regime*, 79 *Wash. U. L.Q.* 491, 491-93 (2001); . None, however, consider a statute’s dependence on gatekeeper liability to be a potential weakness.

<sup>96</sup> One notable exception to this generalization is Randal C. Picker, *Copyright as entry policy: the case of digital distribution*, 47 *Antitrust Bull.* 423, 432 (2002). A similar notion is reflected in the distinction between “broad-based” and “targeted” enforcement in Rick Harbaugh & Rahul Khemka, *Does copyright enforcement encourage piracy?*, Claremont Colleges working paper in economics, Aug. 2001, at <http://econ.mckenna.edu/papers/2000-14.pdf>. One reason copyright’s dependence on gatekeepers may be under recognized is possibly because most of copyright law is found under the civil, as opposed to the criminal titles of the law. Yet there is no reason to suppose from first principles that a civil regime cannot also harness the power of a gatekeeper liability regime.

copyright achieved compliance through the imposition of liability on a limited number of intermediaries: those capable of copying and distributing works on a mass scale. The gatekeepers were book publishers at first, and later record manufacturers, film studios, and others who produce works on a mass scale. They were placed in an equivalent position to doctors with respect to prescription drugs—they prevented evasion of the law by blocking the opportunity to buy an infringing product in the first place.

That intermediaries play some role in copyright enforcement is widely recognized<sup>97</sup>—it could not be otherwise after the Supreme Court’s decision in *Sony Corp. of America v. Universal City Studios*.<sup>98</sup> And writers have hinted at the potential dependence of copyright on a gatekeeper system. As Professor Jane Ginsberg noted in 1995:

Copyright owners have traditionally avoided targeting end users of copyrighted works. This is in part because pursuing the ultimate consumer is costly and unpopular. But the primary reason has been because end users did not copy works of authorship—or if they did copy, the reproduction was insignificant and rarely the subject of widespread further dissemination.<sup>99</sup>

But I am saying something more: In structure and presumption, copyright had become totally dependent on gatekeeper enforcement, relying on its gatekeepers to achieve compliance. The goal of this section is to prove this proposition. Unfortunately, academic study of copyright enforcement is sparse.<sup>100</sup> What we can learn about enforcement patterns comes largely from

---

<sup>97</sup> See, e.g., Jane C. Ginsburg, Putting Cars On The “Information Superhighway”: Authors, Exploiters, and Copyright In Cyberspace, 95 Colum. L. Rev. 1466, 1488 (1995) (discussing the role of intermediaries); Jessica Litman, Digital Copyright 111 (2001) (“Our copyright laws have, until now, focused primarily on the relationships among those who write books of authorship and disseminate those works to the public.”)

<sup>98</sup> 464 U.S. 417 (1984). In the Sony litigation, the broadcasting industry targeted Sony and its new Betamax Video Tape Recorder, as opposed to end-users, when it unsuccessfully tried to have Sony held contributorily liable for any illegal taping of television shows. *Id.* at 456.

<sup>99</sup> Ginsburg, *supra* note 97, at 1488.

<sup>100</sup> While many authors discuss the challenge of new technology for intellectual property laws, it is difficult to find academic work on actual patterns of enforcement. One student note has tackled the problem, relying principally on Congressional sources. See Jayashri Srikantiah, Note, The Response of Copyright to the Enforcement Strain of Inexpensive Copying Technology, 71 N.Y.U. L. Rev. 1634, 1643-45 (1996) (describing the patterns of copyright enforcement).

the few hearings and Congressional studies on copyright enforcement and the case record itself.

Reflecting an interest in bigger targets, copyright maintained an indifference to private, home copying in the 1960s and early 1970s. In 1971 Congress commented that copyright was never meant to “restrain the home recording, from broadcasts or from tapes or records, of recorded performances.”<sup>101</sup> Congress described the practice of non-commercial home recordings as “common and unrestrained.”<sup>102</sup> In the 1973 photocopying case *Williams & Wilkins Co. v. United States*, the United States Court of Claims similarly stated, “it is almost unanimously accepted that a scholar can make a handwritten copy of an entire copyrighted article for his own use . . . . These customary facts of copyright-life are among our givens.”<sup>103</sup>

Even in the 1976 Act, the decision was made to limit the exclusive right of performance of audiovisual works to public performances, thereby excluding private or home performances.<sup>104</sup> In recommending this limit, the Copyright Office explained that “[n]ew technical devices will probably make it practical in the future to reproduce televised motion pictures in the home. We do not believe the private use of such a reproduction can or should be precluded by copyright.”<sup>105</sup> The law’s indifference toward home copying was echoed by a lack of enforcement. The case record is perhaps the strongest evidence of the operation of the old regime. One is pressed to find any example of copyright law being enforced against individuals for home copying (as opposed to commercial activity) prior to 1990. In the 1979 Sony betamax case, copyright owners added a representative individual to the complaint, but they did not seek relief against him.<sup>106</sup> Beyond this limited example, individualized infringement actions were absent until the 1990s.<sup>107</sup>

---

<sup>101</sup> H.R. Rep. No. 92-487, at 7 (1971).

<sup>102</sup> *Id.*

<sup>103</sup> 487 F.2d 1345, 1350 (1973), *aff’d* by an equally divided Court, 420 U.S. 376 (1975).

<sup>104</sup> 17 U.S.C. §106(4) (2000).

<sup>105</sup> Register of Copyrights, 87th Cong., Report of the Register of Copyrights on the General Revision of the U.S. Copyright Law 30 (Comm. Print 1961).

<sup>106</sup> *Universal City Studios v. Sony Corp. of Am.*, 480 F. Supp. 429, 432 (C.D. Cal 1979); see also *Sony Corp. of Am. V. Universal City Studios*, 464 U.S. 417, 434 (1984) (“The two respondents in this case do not seek relief against the Betamax users who have allegedly infringed their copyrights.”).

<sup>107</sup> The 1990s have seen an effort by software copyright owners to enforce copyright against end-users, who tend to be fairly large entities. See, e.g., Elizabeth Hurt, *Software Pirates Sued: Alleged culprits targeted online auction bidders*, *Business 2.0*, Jan. 26,

The Supreme Court's decision in *Dowling v. United States* and decisions like it come closest to primary enforcement against individuals.<sup>108</sup> *Dowling* featured two Elvis enthusiasts who pressed unreleased recordings without permission—bootleggers.<sup>109</sup> But these bootleggers were actually sizable distribution channels. In *Dowling*, the two hobbyists grew to do “substantial business,”<sup>110</sup> and eventually functioned just like regular record-sellers themselves. They printed catalogs and advertisements and sold and distributed thousands of albums.<sup>111</sup> Were these Elvis bootleggers gatekeepers in the enforcement sense? While the *Dowling* defendants were both consumers and distributors of illegally copyrighted works, it remains that the end-users of the Elvis bootlegs would be unable to obtain their product without the cooperation of Dowling and company.

Mass home copying became an issue in the late 1980s and prompted some examination of how copyright enforcement worked.<sup>112</sup> As the Congressional Office of Technology Assessment stated in its 1989 report, “[a]ll U.S. copyright law, including the Copyright Act of 1976, proceeds on the assumption that effective and efficient copying is a large-scale, publicly visible, commercial activity, and therefore, that legal prohibitions against unauthorized copying are enforceable.”<sup>113</sup> This report, echoed by hearings on copyright enforcement in the 1980s, confirmed that the existing pattern of enforcement by the Recording Industry Association of America (RIAA) and the motion picture industry was against large scale commercial pirates.<sup>114</sup> After making clear copyright's long reliance on a gatekeeper system, it is

---

2001, at <http://www.business2.com/articles/web/print/0,1650,16147,00.html>. For an argument that this enforcement actually creates more piracy, see Harbaugh & Khemka, *supra* note 96, at 2.

<sup>108</sup> 473 U.S. 207 (1985). Other examples of enforcement against small intermediaries include *United States v. Drum*, 733 F.2d 1503 (11th Cir. 1984) (bootlegging enterprise), and *Paramount v. Labus*, No. 89-C-797-C, 1990 WL 120642 (W.D. Wis. Mar. 23, 1990) (involving the operator of a small resort sued for renting pirated movies to his customers).

<sup>109</sup> 473 U.S. at 210-11.

<sup>110</sup> *Id.* at 212.

<sup>111</sup> *Id.* at 211-12.

<sup>112</sup> The Office of Technology Assessment noted that the proportion of people who made home audiotapes doubled in the 1980s. See U.S. Congress, Office of Technology Assessment, *supra* note 13, at iii (1989).

<sup>113</sup> *Id.* at 7.

<sup>114</sup> See Civil and Criminal Enforcement of the Copyright Laws: Hearing Before the Subcomm. on Patents, Copyrights and Trademarks of the Senate Comm. on the Judiciary, 99th Cong. 41 (1985) (statement of \_\_\_\_\_) (“RIAA is selective in what they refer to Justice, turning over only the most egregious cases.”).

possible to specify more precisely why the changes of the 1980s and 1990s altered the face of copyright enforcement.

## B. Digitalization & Disintermediation

Gatekeeper regimes have an obvious weakness. They depend on the specialized good or service remaining specialized. For the 270 years following copyright's 1710 debut, this remained the case for copyrighted works: copies could not be produced by just anyone.<sup>115</sup> As demonstrated by the Elvis bootleg case *Dowling*, there could and did arise corruptible publishers who would produce illicit copies (just as corruptible doctors hand out illicit drugs).<sup>116</sup> But so long as the costs of finding such corrupted intermediaries remained reasonable, gatekeeper liability continued to prevent copyright infringement.

Digitalization—the ability to make perfect digital copies of content—was the beginning of a problem for the gatekeeper regime. It put copying certain forms of content within the reach of anyone with a computer. As the Office of Technology Assessment documented in 1989, the extent of an individual's copying power was mainly limited to computer software and analog taping of television programs and music.<sup>117</sup> By the 1990s individual's ability to copy spread to music (with the advent of powerful compression algorithms) and, to some extent, books and film.

It is important to understand that digitalization itself did not mean the end of a gatekeeper system. It put home copying within easy reach. Mass distribution, however, remained (and still remains, for most works) a gate kept by a few. So long as mass distributors of content remain identifiable and easy to sue, the gatekeeper regime can remain effective. Unfortunately for copyright, the mass popularity of the internet in the mid-1990s threatened the existence of precisely these remaining gatekeepers.

What, exactly, about peer designs threatened the gatekeeper regime? The design of peer networks eliminates intermediaries. Their design, at least in theory, creates a distribution network of perfect equals, each of whom is both a consumer and a distributor of copyrighted materials. I will explain, technically, how this is accomplished in a moment. For present purposes, peer designs can be understood as a tool for “de-specializing” the distribution of copyrighted materials.

This creates difficulty for a gatekeeper regime, which depends on targeting visible, specialized intermediaries. From this it is apparent why peer

---

<sup>115</sup> Please provide a citation for this assertion.

<sup>116</sup> See *Dowling v. United States*, 473 U.S. 207 (1985).

<sup>117</sup> See U.S. Congress, Office of Technology Assessment, *supra* note 13, at iii.

networks pose a challenge to copyright enforcement (more generally, network designs that credibly delete intermediaries may threaten a regime dependent on targeting gatekeepers or other intermediaries). A theoretically perfect peer network would have no intermediaries and force copyright to rely exclusively on a primary enforcement model. This copyright has never done before.

This explains why peer filesharing can create trouble for copyright's enforcement system. But how, exactly, was peer filesharing a strategy to reduce the costs of copyright? Unlike a typical criminal prohibition, the imposed costs of the copyright regime can be more complicated to model. Essentially, peer filesharing gives its users the opportunity to bypass the need to obtain content from traditional distribution gatekeepers (music stores) and the many costs thereby associated.

First, sources estimate that for an average CD, manufacturing costs of the CD are \$1, distribution costs are \$1, royalties are between \$1 and \$2, and retailers' profits are \$5 and up.<sup>118</sup> Peer filesharers are able to bypass all of these costs if they are happy with the MP3 version of a given CD. Second, while only indirectly a cost of copyright, filesharers save due to the fact that peer filesharing is an efficient method of distribution. The at-home nature and diversity of offerings on filesharing networks save filesharers the costs of going to music stores and searching for obscure music. Finally, as discussed in greater detail below, peer filesharers can take advantage of these costs savings while continuing to enjoy a system with incentives to create music, so long as their compatriots without computers continue to pay.<sup>119</sup>

### C. Elements of Peer Design

While the total elimination of intermediaries in a "pure" peer design would target the existing structure of copyright enforcement, designers agree that implementing such a large-scale pure peer architecture is a serious challenge.<sup>120</sup> The programmers of a peer response must balance an interest in avoiding legal liability with the competing challenges of ensuring performance on a mass scale, maintaining system stability, and fostering

---

<sup>118</sup> See Robert Burnett, *The Global Jukebox: The international music industry* 91 (1996); Zoonky Lee & Sanjay Gosain, *Price Comparison for Music CDs in Electronic and Brick-and-mortar Markets: Implications for Emergent Electronic Commerce*, in *Proceedings of the 33rd Hawaii International Conference on System Sciences* 3 (2000), at <http://www.computer.org/proceedings/hicss/0493/04936/64936044.pdf>.

<sup>119</sup> See *infra* text accompanying notes 157-160.

<sup>120</sup> For a good summary of some of these challenges, see Theodore Hong, *Performance*, in *Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology* 205-06 (Andy Oram, ed., 2001).



network trust. These matters all require control over the network; while a pure peer design eliminates control as much as possible. A more technical turn will illuminate these points more thoroughly.

The goals of a peer filesharing application are a good place to begin this discussion. Two people can trade files easily, using email or a disk. But what about one million people? The general goal of a peer filesharing network is to enable millions of home users to trade files amongst themselves quickly and easily. Such a program generally requires three elements. First, it requires a program that normal, home users can download; a program that running on their computer can locate other users, creating the networks of peers. Second, it requires some way for each user to search the network (or parts of it) to find out what content others are making available. Finally, it requires some way for users to send the files to each other once they have found something desirable.

These filesharing goals are accomplished using a peer-to-peer design. Formally, a peer-to-peer network is an application architecture where each “node” or computer has equivalent rights and responsibilities.<sup>121</sup>

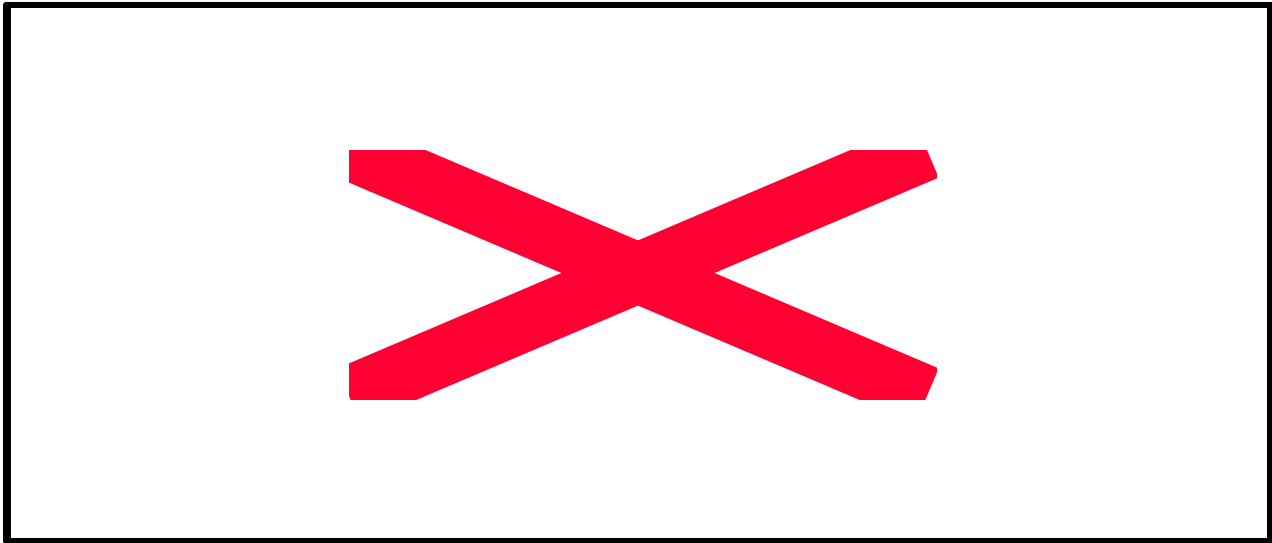


Figure 1. Design of a Peer-to-Peer versus a Server-Client Network

This, as the name suggests, makes it a network of equals, or peers. The network architecture is, classically, distinguished from a “client-server”

---

<sup>121</sup> See Michael A. Gallo & William A. Hancock, *Networking Explained* 11 (1999).

network, in which one computer specializes in serving the needs of others. As the name suggests, a centralized “server” serves the “clients.”

Real-world metaphors help capture this important difference.

Consider the difference between a study group and a lecture room with a teacher. On the one hand, the study group is a peer network. Each member has both the responsibility to share materials and the right to take materials from others. The classroom, on the other hand, is a “server-client” network. The teacher specializes in teaching the students. The students do not teach the teacher or each other. The network is centralized, and each node is specialized.

A pure peer design is “flat” with equal, non-specialized members. Client-server designs are hierarchical, with a specialized server. Each design has its own uses, but only peer networks threaten the gatekeeper structure of copyright enforcement.

#### **D. “Pure” Peer Networks, and Hybrids**

The distinction between peer and server-client designs is fundamental to understanding the challenge of building a network that resists copyright enforcement. The more purely peer-to-peer the network design, the more disparate the targets for copyright infringement, and the greater the threat to a gatekeeper system.

Why not simply always build the most decentralized design possible? The general answer is, it is difficult. Indeed, within the technical community, variations from purity are so commonplace that there are healthy debates over what should even be considered a peer network.<sup>122</sup>

Pure peer networks are a challenge because eliminating intermediaries decreases control over the network. The loss of control makes it difficult to ensure performance at a mass scale, to establish network trust, and even to perform simple tasks like keeping statistics. As networks grow larger, these problems become more important. It is simple, in other words, to build a pure peer-to-peer network for six friends interested in trading, just as a study group with six members is manageable. But the same design will be unlikely to work for ten million or one hundred million people.

In practice, there are four recognized classes of application design, pictured in Figures 1 and 2 and summarized in Table 1. Figure 1 pictures the

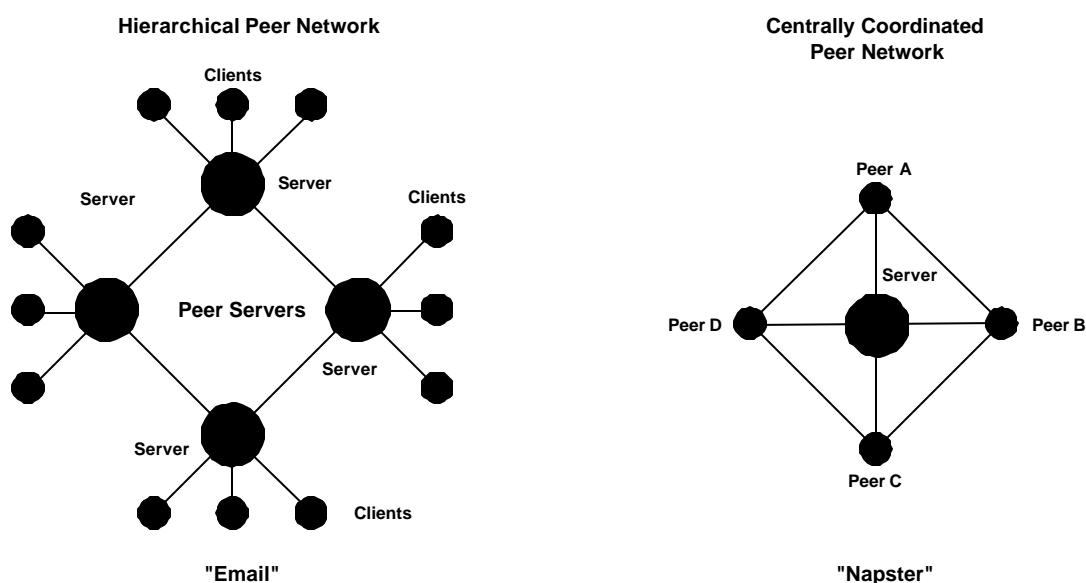
---

<sup>122</sup> See, e.g., Gene Kan, Gnutella, *in* Peer-to-Peer, *supra* note 120, at 117; Clay Shirky, What is P2P... And What Isn't?, at <http://www.oreillynet.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html> (Nov 24, 2000).

two extremes. The client server model is typical of the Internet's most important application, the World Wide Web. The "pure" peer design, meanwhile, is what the early version of the Gnutella peer filesharing program adopted to avoid infringement liability.

It is often useful in a peer design to have at least one central server, to store user information, search databases, and trust information. Such a design forms the "centrally coordinated" peer network, pictured on the right of Figure 2. Napster used this architecture, as do popular chat programs like AOL Instant Messenger.<sup>123</sup>

Figure 2: Hybrid Designs



Finally, some of the best designed networks balance control and decentralization carefully. They appear peer-to-peer to the end-users but are actually peer-to-peer between specialized servers. This "hierarchical peer-to-peer" design, pictured on the left of Figure 2, lies behind regular IP email, the Domain Name System (DNS), and the classic newsreader "usenet."<sup>124</sup> With email, no central authority controls delivery of emails. Rather, a particular

<sup>123</sup> See Nelson Minar et al, A Network of Peers, *in* Peer-to-Peer, supra n. 138, at 17.

<sup>124</sup> See RFC 1036, available at <http://www.ietf.org/rfc/rfc1036.txt> (detailing structure of usenet system).

university or company's servers communicate with other institutional servers in a peer-to-peer fashion.<sup>125</sup>

Table 1: Types of Network and Examples

Network Type	Example
Client-Server	World Wide Web
Centrally Coordinated Peer Network	Napster, Instant Messenger
Hierarchical Peer Network	Email, Usenet, DNS
Pure Peer Network	Gnutella

In practice, what is called a peer network may be peer only in certain respects. To understand the challenge, it is helpful to examine the life cycle of a node in a peer network, and observe how often intermediaries will appear. Every intermediary, of course, is a potential legal target.

#### *Step 1. Getting Software & Finding Peers*

To begin life as a peer node, the appropriate software needs to be installed by the user. This usually means downloading from some intermediary (typically someone's web site).

The node must find at least one peer to join the peer network. But how can this be done without knowing anything in advance? Again, the solution is usually reliance on some intermediary, such as a "host cache" that starts the peer node with one peer address to begin.

#### *Step 2. Discovering Peer Content – The Search Function*

---

<sup>125</sup> See RFC 1035 <http://www.ietf.org/rfc/rfc1035.txt> (detailing design of domain name system).

To be useful, the peer node requires some ability to discover what content is available on the network. For example, in a network meant to share music, users need to know what songs are actually available, preferably searching by artist, title, etc. The very volume of search traffic thus generated, however, can strain a network design to the point of collapse.<sup>126</sup> This is mitigated if the network is designed to access a finite amount of content (for example hit songs). Nonetheless, this remains a fundamental challenge.

It is easiest to store search information in one place. If search information is centralized, as in the Napster design, it creates yet another specialized intermediary.

### *Step 3. Transmitting Information Between Peers*

Finally, peer networks need to provide for connections among peers. Here, the greatest problems for non-centralized peer models come from user abuse of anonymity. In a music network, copyright owners could potentially send around fake files. In network terms, this is the problem of “trust.” From first principles it is clear that trust systems are difficult if not impossible to create without some centralized system of verification.

The elimination of intermediaries is a serious challenge. It forces designers to compromise. The less intermediaries, the fewer targets for an infringement lawsuit. Fewer intermediaries, however, make it harder for users to use the system and increase the risk of system crashes and anonymous attacks. Writing a successful peer application requires a delicate balancing of these competing concerns.

Having concluded the study of how the peer network response targeted copyright’s gatekeeper enforcement regime, it is now possible to consider its interaction with norms concerning theft.

## **E. Copyright and Social Norms**

Seventy-eight percent of those who download music do not consider it to be stealing, according to a 2000 Pew study, and 61% do not care if the music they download is copyrighted.<sup>127</sup> These statistics suggest that peer filesharing’s design not only undermines copyright’s gatekeeper regime, but

---

<sup>126</sup> See, e.g., Gene Kan, Gnutella, *in* Peer-to-Peer, *supra* note 120, at 112-114.

<sup>127</sup> See Amanda Lenhart et al., Downloading Free Music: Internet music lovers don’t think it’s stealing, The Pew Internet & American Life Project’s Online Music Report September 28, 2000, at 5, available at <http://www.pewinternet.org/reports/toc.asp?Report=23>.

also successfully sidesteps social norms that might otherwise bolster compliance with the copyright regimes.

As discussed above, theorists have suggested that the possibility of state punishment provides an incomplete explanation for observed compliance with societal rules.<sup>128</sup> Rather, they suggest that other systems of social control, including the system of social norms, account for the compliance observed.<sup>129</sup> While accounts differ, the arguments hold that either the threat of external social sanctions,<sup>130</sup> the fear of sending the wrong signals to others,<sup>131</sup> or the internalization of ethics<sup>132</sup> make people comply with the rules to a degree that exceeds a simple reaction to the threat of punishment.

Those who benefit from copyright benefit from the fact that physically stealing a CD or DVD is socially unacceptable. They are hurt, however, by the norm that makes copying the same CD at home acceptable. Economically each is approximately the same loss of a potential sale (assuming a similar likelihood that the thief or friend would have otherwise paid the full price for the music).

For these purposes, rather like the gatekeeper regime just described, the system of social norms is an alternative mechanism of creating compliance with a given legal rule. If norms tend to track the substance of legal rules, it stands to reason that a rational, mass effort to reduce the costs of regulation must somehow sidestep the enforcement of legal rules through the system of social norms. If, for some reason, it were considered disgraceful and perverse to download music on the internet, copyright compliance could be achieved without active, primary enforcement. However, peer filesharing successfully exploits the status of norms surrounding copyright, taking full advantage of an existing ambiguity as to whether home, non-commercial copying is “wrong.”

In one of the few disinterested studies of its time, the Congressional Office of Technology Assessment in 1989 surveyed attitudes toward home

---

<sup>128</sup> See sources cited *supra*, n. 25.

<sup>129</sup> Understanding exactly how norms operate to ensure compliance with legal rules is beyond the scope of this paper. For a new account of this issue see Mahoney & Sanchirico, *supra* note 128 (manuscript at 41-48) (suggesting that the state’s punishments play a role in sustaining strategies of cooperation with legal rules).

<sup>130</sup> A classic external sanction model is provided in Ellickson, *supra* note 128, at 124-26.

<sup>131</sup> The signaling theory is presented in Eric Posner, Symbols, Signals, and Social Norms in Politics and the Law, 27 *J. Legal Stud.* 765, 766-67 (1998).

<sup>132</sup> See Robert D. Cooter, Decentralized Law for a Complex Economy: The Structural Approach to Adjudicating the New Law Merchant, 144 *U. Pa. L. Rev.* 1643, 1661-66 (1996) (taking internalization as the precondition of a norm’s existence).

copying.<sup>133</sup> The study found a simple norm: people think copying for friends is okay, but copying for money is wrong.<sup>134</sup> More precisely, it found that large majorities (63%) of consumers considered making a taped copy of audio materials for a friend to be “acceptable” or “perfectly acceptable.”<sup>135</sup> On the other hand, the public (76%) found selling copied materials unacceptable.<sup>136</sup> The survey mirrors widespread anecdotal evidence,<sup>137</sup> suggesting a normative difference between commercial and non-commercial copying.

P2P exploits this distinction brilliantly. P2P clients create no sensation or impression of stealing; an instance of what Lior Strahilevitz would call “charismatic code” design. Instead, the user is invited to a “community” of peers who exchange song files. There is, importantly, no sense of a sale of copyrighted materials. The design therefore seems to operate at the gap between acceptance of non-commercial copying and non-acceptance of commercial copying. While its economic consequences could be large, the lack of commercial exchange in its operation seems to make filesharing acceptable under the norms of home copying.

**Fig. 1: The Friendly Face of the Bear-Share Community**

---

<sup>133</sup> See U.S. Congress, Office of Technological Assessment, *supra* note 112, at 139-65.

<sup>134</sup> *Id.* at 163.

<sup>135</sup> *Id.*

<sup>136</sup> *Id.*

<sup>137</sup> Jessica Litman, for example, argues that in general people “do not observe copyright rules in their daily behavior,” because “people don’t believe the copyright law says what it does say.” Litman, *supra* note 97, at 111-112.



As just one example, consider the BearShare client pictured above. There is little on the screen to suggest a sketchy operation or an act of theft. Indeed, the Bear in BearShare is the perfect embodiment of charismatic code.

The side-step of social norms seems to have succeeded. The 2000 Pew Survey clearly supports the view that those who use filesharing networks overwhelmingly do not think they are stealing.<sup>138</sup> That same study also suggests that 53% of all Internet users, and even 40% of Americans, think that by sharing music through the internet they are not doing anything wrong.<sup>139</sup> A 2002 survey by the Business Software Alliance, similarly, found only 38% of Internet users claimed they would never download a potentially pirated program to save money.<sup>140</sup>

In the end, then, P2P not only exploits the limits on legal enforcement, but also manages to dodge the system of social norms that usually follow legal rules.

\* \* \*

This Part has shown that P2P depends on certain vulnerabilities of copyright's to achieve avoidance. The next Part considers the reaction of the beneficiaries of copyright, and the ensuing regulatory competition.

<sup>138</sup>Lenhart, *supra* note 127, at 5.

<sup>139</sup> *Id.* at 6.

<sup>140</sup> See Business Software Alliance, *Survey Spotlights Growing Problem of Online Software Piracy* (2002), at [www.bsa.org](http://www.bsa.org).



## Part II: The Evolution and Regulatory Competition

The years 1999 to 2003 witnessed a regulatory competition between P2P users and the incumbent industry. At stake was an obvious rents: the monopoly rents possible obtainable when the copyright law is enforced. As the succeeding narrative shows, the two groups had different comparative advantages: the one code, the other litigation, and legal change. In other words, the competition pitted methods of avoidance against methods of change in a direct competition.

There are two outstanding aspects of this story. The first is the degree to which code design evolved to better target the weaknesses of the copyright regime. In the previous section, we saw that P2P was generally designed to target copyright's dependence on a gatekeeper system and its lack of normative support. Here we see code design evolving to take advantage of a specific legal doctrine: copyright's contributory liability doctrine, embodied in the *Sony* decision.

Peer filesharing networks appear to be very intelligently crafted tools for exploiting the weaknesses of copyright's enforcement system. But the history of their development reveals no such centralized vision. Rather, in the main, the development of peer filesharing is marked by uncoordinated projects growing out of the ruins of earlier failures.

Finally, the development story also shows an evolutionary pattern: a very few successful programs against a much larger background of failures. Over the years 1999-2002 inclusive of development, there were approximately fifty-eight different filesharing clients released to the market.<sup>141</sup> Of those, only four or five have gained lasting significance.<sup>142</sup>

### *Napster and its Predecessors*

---

<sup>141</sup> The compiled list of filesharing clients from 1999-2002 includes: Abe's MP3 finder, Ares, Audio-Galaxy, AudioGnome, Aimster (now named Madster), BadBlue, Bearshare, Blubster, CuteMX.Com, DirectConnect, eDonkey, Filetopia, File Navigator, FileAngel, File Rogue, FileSpree, Free Haven, Freenet, Frost, Grokster, Gnutella, Gnucleus, Gnutella 0.56, Gnutmeg, Groove Network, Hotline Communications, iMesh, iSwipe, Junge Monkey, MyNapster, KaZaa, KonSpire, Limewire, Mactella, Mojo Nation, Morpheus, Myster, Napster, NapMX, Nutella, Ohaha, OpenNap, Phex, Phosphor, Pointera, Publius, Qtella, OnSystem, Qube, Scour.com, Shareaza, Spinfrenzy, SongSpy, Taxee, Voodoo Vision, WinMX, Xolox. Of course, many of these are clients for the same networks, as in the multiple GnutellaNet and FastTrack clients.

<sup>142</sup> In focusing on the major developments, some might argue that I have shortchanged programs like Scour.com and Aimster in the process.

While Napster was the first laboratory for a peer response, it was itself a reaction to an earlier model. The very first efforts at mass distribution of copyrighted materials employed a purely client-server model—essentially, web sites with songs for download. The company “MP3.com,” which debuted in 1996, is a well-known example. Among other things, its “My.MP3” service allowed users to download copyrighted MP3 files, provided they owned the CD that corresponded to the file in question.<sup>143</sup> This service was meant to give users remote access to music that they already owned.

The architecture of My.MP3 and other web-based services is of particular interest here, not the fair-use issue.<sup>144</sup> My.MP3 relied on a pure client-server model. It copied a huge amount of copyrighted materials and placed them in a single place. When the recording industry sued, the company’s activities easily fit into the traditional model of copyright enforcement.<sup>145</sup> The recording industry’s case was not much different, enforcement-wise, from the Elvis bootleggers in *Dowling v. United States*<sup>146</sup>—both were large, centralized copiers of copyrighted materials.

Other sources of copyrighted sounds in the early 1990s were the primitive, anonymous websites that simply made MP3s available for download.<sup>147</sup> But these sites faced two serious technological problems. First, if a site became popular it would quickly become overburdened with user traffic. Second, there were few reliable and straightforward means for finding such sites.<sup>148</sup>

Then came Napster. The beta version of Napster debuted on June 1, 1999. Napster’s revolutionary design was a response to the legal and technical problems of the web-based companies. As one commentator noted, “[Napster] was written to solve a problem—[legal] limitations on file copying.”<sup>149</sup>

---

<sup>143</sup> See Lawrence Lessig, *The Future of Ideas* 192 (2001).

<sup>144</sup> Since MP3.com required users to own the CD for the mp3s they were given the right to download, there was a good argument that MP3.com’s copying of the files to facilitate “space-shifting” was fair use. See Lawrence Lessig, *The Future of Ideas* 192-93 (2001).

<sup>145</sup> See *UMG Recordings v. MP3.com*, 92 F. Supp. 2d 349, 350 (S.D.N.Y. 2000).

<sup>146</sup> See 473 U.S. 207 (1985).

<sup>147</sup> See Bruce Haring, *You can't stop the music on the Net* Recording industry debates MP3 piracy issue, *USA Today*, Nov. 4, 1998, at 1998 WL 5740934 (noting the “abundance of sites both legal and illegal”).

<sup>148</sup> For example, the web site MP3Board offered a search engine for such sites, and was quickly sued. See *MP3Board v. Recording Indus. Ass'n of Am.*, No. C-00-20606 RMW, 2001 WL 804502, \*3 (N.D. Cal. Feb. 27, 2001) (staying a California countersuit).

<sup>149</sup> Shirky, *supra* note 122, at 28.

Napster eliminated the intermediary that had doomed My.MP3 and others. It designed a network that decentralized the infringing content, leaving the songs on the hard drives of individual home users. Napster made itself different from the traditional commercial copyright pirate. It styled itself a place to trade music. It did not sell or distribute music.

Napster was not completely decentralized. Napster's programmer Jordan Ritter was keenly aware of the challenge of operating on a mass scale.<sup>150</sup> Napster mixed client-server and peer elements in order to make the search for songs a fast and scalable solution. Hence, the search database and the brokering of individual connections were both performed by the Napster server.

The design scaled impeccably. At its height, while estimates vary, Napster could count tens of millions of active users, an astonishing technological accomplishment.<sup>151</sup> But the failure to remove itself as an intermediary with control over parts of the process made Napster, the company, a target for an infringement lawsuit. That lawsuit came on December 6, 1999.<sup>152</sup>

The infringement case against Napster boiled down to a question of control, intimately connected to the network design questions studied here. The situation would be different if Napster had been a sort of multi-purpose copying technology, over which Napster had no specific power. This would have put Napster in the same position as cameras, VCRs, and other forms of "copying equipment" described in *Sony Corp. of America v. Universal City Studios*.<sup>153</sup> The makers of VCRs and photocopiers obviously know that their products are often used to infringe copyright. But since they are powerless to do anything about these violations, and the equipment has substantial non-infringing uses, they are not made liable.<sup>154</sup>

Napster's argument—that it was a mere instrument of both legal and illegal uses—was betrayed by its design. One factual finding doomed the company. The court found that "[Napster] could block access to the system by suppliers of the infringing material."<sup>155</sup>

---

<sup>150</sup> See Jordan Ritter, *Why Gnutella Can't Scale. No Really.* (2001) available at <http://www.darkridge.com/~jpr5/doc/gnutella.html> (discussing scaling problems in P2P networks).

<sup>151</sup> See Healy, *supra* note 86.

<sup>152</sup> See *A&M Records v. Napster*, 114 F. Supp. 2d 896, 900 (N.D. Cal. 2000).

<sup>153</sup> 464 U.S. 417, 442 (1984) ("[T]he sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes.").

<sup>154</sup> The *Sony* court described this as the "staple article of commerce doctrine." *Id.*

<sup>155</sup> *A&M Records*, 239 F.3d at 1022; see also *id.* at 1023 ("The district court correctly determined that Napster had the right and ability to police its system.").

This fact made Napster the sponsor, rather than just the instrument, of infringing conduct. Instead of a VCR, Napster's design put it in the classic position of the dance hall that chooses to allow an infringing artist to play, despite having the power to stop the performance.<sup>156</sup> The *Sony* Court itself declared that when a defendant is "in a position to control the use of copyrighted works by others," the "imposition of vicarious liability is manifestly just."<sup>157</sup>

After finding control, holding Napster to be both a contributory and a vicarious infringer was easy. Napster's design allowed the record industry to use the notice and failure to remove formula to prove knowledge (an element of contributory copyright infringement).<sup>158</sup> The record industry sent Napster notice of thousands of infringing files available through the system, and then proved that these files were still available to be downloaded later.<sup>159</sup>

On the redundant issue of vicarious liability, the decisive legal question was also that of control. As the appeals court framed it, the question was whether Napster had "the right and ability to supervise the infringing activity and also ha[d] a direct financial interest in such activities."<sup>160</sup> Napster's architecture again provided an answer. As the court noted, "Napster retains the right to control access to its system."<sup>161</sup>

This ruling eliminated Napster's specific relevance as a response, and ultimately led the company to bankruptcy.<sup>162</sup> But Napster taught several legal lessons to the designers of the peer response. As the late Gene Kan, a post-Napster developer, wrote, "[T]he recording industry [] is sensitizing software developers and technologists to the legal ramifications of their inventions.

---

<sup>156</sup> The classic dance hall case is *Dreamland Ball Room v. Shapiro, Bernstein & Co.*, 36 F.2d 354, 355 (7th Cir. 1929) (holding a dance hall liable for copyright infringement because they hired an infringing orchestra to supply music to paying customers). In contrast, landlords have traditionally not been held liable for the infringements of their tenants. See e.g., *Deutsch v. Arnold*, 98 F.2d 686, 688 (2d Cir. 1938) (refusing to hold a landlord liable for the copyright infringement committed by a tenant on the premises).

<sup>157</sup> *Sony*, 464 U.S. at 437.

<sup>158</sup> *A&M Records*, 239 F.3d 1004, 1020 (9th Cir. 2001). This formula that has become the favored technique for proving knowledge in service provider cases. See *Religious Tech. Ctr. v. Netcom On-Line Comm'n Serv.*, 907 F. Supp. 1361, 1373-75 (N.D. Cal. 1995) (allowing actual knowledge to be demonstrated in this manner).

<sup>159</sup> *A&M Records*, 239 F.3d at 1022.

<sup>160</sup> *Id.*

<sup>161</sup> *Id.* at 1023.

<sup>162</sup> The Ninth Circuit's ruling on the preliminary injunction was the effective, but not the formal, end of the Napster litigation. See *A&M Records, Inc. v. Napster, Inc.*, 284 F.3d 1091, 1099 (9th Cir. 2002) (affirming the district court's preliminary injunction).

Napster looked like a pretty good idea a year ago, but today Gnutella and Freenet look like much better ideas. . .”<sup>163</sup> Napster taught peer network designers that both lack of control and general function had to be comprehensive and credible to avoid contributory liability. The relationship between developers and peer networks needed to be more like that between Xerox and its photocopiers. The response, this suggested, should take the form of a protocol rather than an application. Email and Usenet have never been sued for copyright infringement, despite widespread use for illegal purposes. The lesson was simple—Napster had not gone far enough.

There were a flurry of attempts to succeed Napster, many technologically unsuccessful (Napigator) or so clearly liable under *A&M Records* (Scour) as to be unworthy of discussion. But one successor was different. It was founded on concepts of radical decentralization and clearly designed to avoid the copyright lawsuit that had befallen Napster. That successor was the protocol named Gnutella.

## **B. Early Gnutella: 2000-2001**

“Before [Gnutella], systems were centralized and boring.”<sup>164</sup>

Gnutella was a child of the open-source movement. Its unusual name, non-linear development origins, and relative difficulty of use are all hallmarks of an open-source work product.<sup>165</sup> Gnutella delivered a radically decentralized design that made it a darling of academic study. The design was an intentional effort to create a file-sharing protocol that could avoid suit. It succeeded in this goal. Instead, Gnutella’s problems were social and scale related.

Gnutella’s decentralization was nearly complete. No single node on the early Gnutella networks was different than any other. Searching, file transferring, and finding peers were accomplished without the creation of specialized intermediaries. The only identifiable intermediaries were the

---

<sup>163</sup> Gene Kan, Gnutella, *in* Peer-to-Peer, *supra* note 120, at 121.

<sup>164</sup> *Id.*

<sup>165</sup> Gnutella was released on March 22, 2000. It was invented by Justin Frankel and Tom Pepper, two programmers working for AOL’s Nullsoft. Gene Kan, Gnutella, *in* Peer-to-Peer, *supra* note 120, at 95. AOL quashed the effort, but Gnutella’s cause was picked up by the open source movement. See Andy Oram, Gnutella and Freenet Represent True Technological Innovation, Web Review, at <http://www.oreillynet.com/pub/a/network/2000/05/12/magazine/gnutella.html> (May 5, 2001). Its full development followed (and still follows) the non-linear path characteristic of open source. *Id.*

relatively limited number of sites that made the early Gnutella client (version 0.56) available for download.

Gnutella developers compare the network they designed to a cocktail party, where users trade files with whoever happens to be nearby.<sup>166</sup> The design implements the idea that “Gnutella is a protocol, not a program.”<sup>167</sup> In other words, Gnutella’s designers created a file-sharing network—the GnutellaNet—unowned and uncontrolled, to which various Gnutella programs provide access. It is similar to the way various email programs (Eudora, Microsoft Outlook, Hotmail) all give access to the same email network, which cannot be said to be owned by anyone. The GnutellaNet was designed as a general file-sharing network, capable of sharing any computer file.<sup>168</sup>

On the legal front, Gnutella was a success. Gnutella’s radical decentralization achieved the goal of avoiding the legal liability that had plagued Napster. To date, neither GnutellaNet nor its main application designers have been sued,<sup>169</sup> despite the substantial volume of infringement they facilitate.

Instead, the early GnutellaNet was plagued by stability and performance problems attributable to its decentralized design. In late July of 2000, the Gnutella network underwent its first major crash, leaving the network unusable for more than a month.<sup>170</sup> The 2000 crash was the first sign

---

<sup>166</sup> See Gene Kan, Gnutella, *in* Peer-to-Peer, *supra* note 120, at 97-986.

<sup>167</sup> This is a common description of Gnutella. See e.g., From Strategic Vision to a 10-Point Tactical Plan, available at <http://economicdemocracy.org/counterspinners.html> (“Gnutella is not a program, it is a protocol.”).

<sup>168</sup> This characteristic was even more evident in another network, FreeNet, which aimed at achieving the goals of the World Wide Web (storage of information) in a decentralized, purely peer-to-peer fashion. A discussion of the methods used by FreeNet can be found in Ian Clarke et al., Freenet: A Distributed Anonymous Information Storage and Retrieval System, *in* Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability (H. Federrath ed., 2001); see also Adam Langley, Freenet, *in* Peer-to-Peer, *supra* note 120, at 123 (describing the development and structure of Freenet).

<sup>169</sup> It is true that Morpheus switched to Gnutella after it was sued as one of the three FastTrack companies. But no Gnutella developer qua Gnutella developer has been sued.

<sup>170</sup> See Steve McCannell, The Second Coming of Gnutella, Web Review, Mar. 2, 2000, at [http://www.webreview.com/mmedia/2001/03\\_02\\_01.shtml](http://www.webreview.com/mmedia/2001/03_02_01.shtml) (detailing reasons for the crash). Interestingly, the crash came directly in the wake of the Napster injunction on July 26, 2000 as millions of Napster users attempted to migrate to Gnutella. *Id.* The crash provided a dramatic demonstration of the difference in scaling capabilities between the two approaches.

that the early Gnutella client design had traded resistance to litigation for system instability.

Commentators quickly diagnosed the problem.<sup>171</sup> Early GnutellaNet's stability relied on user's willingness to donate both bandwidth and music files to a common cause, and to judiciously limit one's own use of the network. But stark differences in user bandwidth and the lack of a central mechanism for allocating traffic to more capable users made a crash inevitable once a certain number of users joined the network. While some touted the theoretical scaling capabilities of Gnutella,<sup>172</sup> the fact that early GnutellaNet was unstable cannot be denied. Behind the scaling problem also lay "social" problems. There was no incentive (not even social incentives, given the anonymous nature of the network) to act selflessly. A 2000 Xerox/PARC study established that almost 70% of Gnutella users shared no files, and nearly 50% of all responses were returned by the top 1% of sharing hosts.<sup>173</sup> While this did not necessarily matter if the goal was trading the 100 most popular songs, Napster's deeper appeal had been the range of content it made available. The lack of any mechanism to police selfishness in Gnutella compromised the potential of the common solution.

The problems of Gnutella 2000 were generally recognized.<sup>174</sup> Yet Gnutella's failures were not the end of the peer file-sharing response. Instead, the crashes and instability led to a new generation of peer file-sharing software. These new generation programs, bearing names such as KaZaA, Grokster, Morpheus, and Bearshare, are for now the final chapter of the peer response story.

### **C. KaZaA, FastTrack and Superpeers: 2001 - Present**

---

<sup>171</sup> See *id.*; Matei Ripeanu, Peer-to-Peer Architecture Case Study: Gnutella Network, *in* 2001 IEEE International Conference on Peer-to-peer Computing (2001) (describing Gnutella's scaling problems); Jordan Ritter, Why Gnutella Can't Scale. No, Really., at <http://www.darkridge.com/~jpr5/doc/gnutella.html> (Feb. 2001); see also Hong, Performance, *in* Peer-to-Peer, *supra* note 120, at 206-07 (summarizing a now unavailable Clip2 study of the crash). A network engineer would diagnosis the problem as follows: Gnutella's layer 7 topology did not map carefully to the physical network, meaning the network failed to make use of resources available.

<sup>172</sup> Gene Kan, for example, argued that Gnutella would scale perfectly well, and that the 2000 crash was caused by an inappropriate add-on technology. Kan, Gnutella, *in* Peer-to-Peer, *supra* note 120, at 109-17.

<sup>173</sup> Eytan Adar & Bernardo A. Huberman, Free Riding on Gnutella, 5 First Monday, Oct. 2000, at [http://www.firstmonday.dk/issues/issue5\\_10/adar/index.html](http://www.firstmonday.dk/issues/issue5_10/adar/index.html).

<sup>174</sup> See McCannel, *supra* note 171; Ripeanu, *supra* note 171; Hong, *supra* note 120, at 206-07.

The legal vulnerabilities of Napster and the stability and social problems of Gnutella inspired a compromise approach. A new generation of peer-sharing applications tried to strike a balance between suability and scalability. Unlike the original Gnutella, they allowed some hierarchy and made some effort to engineer polite behavior. At the same time, they tried to avoid the centralized control that was Napster's downfall.

The new generation reintroduced hierarchy among users. They created a distinction between "regular peers" and "super peers," based on detected resources—in particular, bandwidth.<sup>175</sup> In this hierarchy, college students are on top: high bandwidth users (college students on university networks, home DSL, and cable users) are super peers, while dial-up users (home modem users) are regular peers.

Dozens of programs grew into the technological gap between Napster and Gnutella. Only a very few, however, reached mass scale for any length of time.<sup>176</sup> The focus of this section is on the main group that abandoned Gnutella altogether for a proprietary protocol named FastTrack, along with the continued development of Gnutella.

#### *FastTrack & KaZaA*

FastTrack returned mass scale to filesharing. In late 2001 the FastTrack network grew to be the largest file-sharing network since Napster, with an average of two to four million users online at any time.<sup>177</sup> Dutch programmers Niklas Zennstrom and Janus Friis created the FastTrack protocol late in 2000, and wrote a client application, KaZaA, to access the FastTrack network.<sup>178</sup> Unlike Gnutella, the protocol was never released as an open-source standard.<sup>179</sup> Instead, KaZaA insisted that companies pay to

---

<sup>175</sup> Names vary: Bearshare groups users into "ultrapeers" and "leafs." See Bearshare, Gnutella Good Citizen Tips, at <http://www.bearshare.com/help/citizen.htm> (last visited February 9, 2003).

<sup>176</sup> Some of the more major programs from this period not discussed here include Audio-Galaxy, Aimster (now named Madster), WinMX, iMesh, and OpenNAP.

<sup>177</sup> This number is based on Active Users Atatistics, at [www.sylk.com](http://www.sylk.com) (July 22 – August 8, 2002).

<sup>178</sup> Kevin Maney, Fight over digital music file-sharing keeps getting weirder, USA Today, September 25, 2003 at B3.

<sup>179</sup> It has been reverse-engineered by several groups, who create clients that access the FastTrack network without permission. A prominent example is giFT (giFT Isn't FastTrack). See generally What is the giFT project?, at <http://gift.sourceforge.net/docs.php?document=whatis.html> (Sept. 14, 2002).



access the FastTrack network. The companies Grokster and Morpheus<sup>180</sup> did so, creating several client alternatives.

The FastTrack companies are somewhere between early-Gnutella and Napster in their elimination of intermediaries. The protocol borrows heavily from Gnutella. It maintains the distinction between the protocol and the clients; the company KaZaA, for instance, maintains no power to “shut down” the network.<sup>181</sup>

FastTrack deviates from the pure design of early Gnutella in several significant ways. First, it implements a very sophisticated system of superpeering designed to avoid scaling problems. This system has been a success. The KaZaA superpeer system, based on popularity and user accounts, provides better performance than even next-generation Gnutella clients.<sup>182</sup> Yet it means that not all users are equal; a finite number of superpeers do the bulk of the work.

Second, the FastTrack companies have, like Napster, centralized several functions. A central server is still responsible for maintaining user registrations, logging users into the system (in order to maintain statistics), and helping the process of finding peers in the first place.<sup>183</sup> As previously discussed, efficient operation and radical decentralization are difficult to maintain.

Third, at least one of the FastTrack companies (KaZaA) engineers selfless behavior, by sharing user files without telling the user. A 2002 Hewlett Packard study demonstrated that the KaZaA client made it difficult to know what files users were sharing.<sup>184</sup> The study demonstrated, in fact, that many users were sharing all the files on their computers, but were totally

---

<sup>180</sup> See Benny Evangelista, *Morpheus software morphing*, S.F. Chron., March 14, 2002, at B1, available at 2002 WL 4015402. Morpheus later reverted to Gnutella, after licensing disagreements with KaZaA. See *id.*

<sup>181</sup> See Amy Harmon, “Music Industry in Global Fight on Web Copies,” N.Y. Times Oct. 7, 2002.

<sup>182</sup> See, e.g., *Morpheus 2.0 – Revisited*, August 19, 2002 <http://www.slyck.com/newsaug2002/081902b.html> (discussing loss of performance when morpheus switched from FastTrack to Gnutella network);

<sup>183</sup> Complaint at 8-9, *Metro-Goldwyn-Mayer Studios v. Grokster*, (No. Civ.01-8541) (C.D. Cal.) (filed October 2, 2001) (seeking damages and injunctive relief for copyright infringement), available at

<http://news.findlaw.com/cnn/docs/mgm/mgmgrokster100201.pdf>.

<sup>184</sup> Nathaniel S. Good & Aaron Krekelberg, *Usability and privacy: a study of Kazaa P2P file-sharing*, HP Laboratories (2002), at <http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf>.

unaware of that fact.<sup>185</sup> Increasing the number of shared files, of course, improves the performance of the network.

Finally, the FastTrack companies also adopted another avoidance strategy: jurisdictional exit.<sup>186</sup> KaZaA's parent is incorporated in Vanuatu, a group of islands in the South Pacific, notable for its lack of a copyright law.<sup>187</sup> Grokster maintains its servers in Nevis, a thirty-six-square-mile nation state in the West Indies.<sup>188</sup> Only Morpheus resides in the United States.<sup>189</sup>

Abandoning decentralization led to a predictable result. On October 2, 2001, the music industry sued the three principal FastTrack companies.<sup>190</sup> The RIAA's complaint takes full notice of the various concessions to centralization previously discussed. Accusing the companies of creating "a 21st century piratical bazaar," the complaint notes that the defendants grant access to "a closed computer network, controlled by Defendants."<sup>191</sup> It also puts considerable emphasis on the fact that communications are centrally encrypted.<sup>192</sup> The complaint recruits these facts to show that the FastTrack companies "are capable of controlling the activities of their users."<sup>193</sup> Most recently, a federal district court found personal jurisdiction over Sharman Networks, the present operator of KaZaA.<sup>194</sup>

#### *Next-Generation Gnutella*

---

<sup>185</sup> Id.

<sup>186</sup> See Amy Harmon, "Music Industry in Global Fight on Web Copies," N.Y. Times, Oct. 7, 2002.

<sup>187</sup> See id.

<sup>188</sup> See id..

<sup>189</sup> See id.

<sup>190</sup> Complaint at 2, 8, Metro-Goldwyn-Mayer Studios v. Grokster, (No. Civ.01-8541) (C.D. Cal.) (filed October 2, 2001) (seeking damages and injunctive relief for copyright infringement), available at <http://news.findlaw.com/cnn/docs/mgm/mgmgrokster100201.pdf>.

<sup>191</sup> Complaint at 2, 8, Metro-Goldwyn-Mayer Studios v. Grokster, (No. Civ.01-8541) (C.D. Cal.) (filed October 2, 2001) (seeking damages and injunctive relief for copyright infringement), available at <http://news.findlaw.com/cnn/docs/mgm/mgmgrokster100201.pdf>.

<sup>192</sup> Id. at 2-3.

<sup>193</sup> Id. at 10.

<sup>194</sup> Metro-Goldwyn-Mayer Studios v. Grokster, No. Civ.01-8541, 2003 WL 186657, at \*15 (C.D. Cal. Jan. 9, 2003) (order denying motions to dismiss).

GnutellaNet, meanwhile, continued to operate on a smaller scale. Recall that neither GnutellaNet nor any Gnutella client has ever been sued – their problems are, instead, self-generated. This fact remains to the present day. Gnutella responded to its scaling and social problems by adapting a superpeer design similar to FastTrack. The best known of the new GnutellaNet developers are Bearshare and Limewire. Both compromise a purely decentralized design by distinguishing between high and low bandwidth users. That is their only concession.

The continued growth of Gnutella was marked by lack of coordination among developers. As Kelly Truelove wrote, “[u]nfortunately, Gnutella has a history of aborted, failed or poorly supported attempts to unite developers; the analogy of herding cats has rarely been so apt.”<sup>195</sup>

Major Gnutella clients have also taken measures to “engineer good behavior.” For example, Bearshare and Limewire block requests from clients who do not contribute files to the GnutellaNet.<sup>196</sup> These efforts, as was the case with the FastTrack companies, may make these clients easier to sue, by facilitating the claim that Bearshare and others “control” the Gnutella network.

Finally, despite the change, Gnutella still appears to have scaling problems of some kind. Statistics kept by Limewire show that, during the year 2002, the network size rarely reached more than 500,000.<sup>197</sup> By July 2002, GnutellaNet had declined to an average of 160,000 nodes.<sup>198</sup> Gnutella experts point to the same general problem: no control over selfish behavior. An anonymous source at Limewire explained the problem: “Client ‘A’ may excessively query (hammer) three or more UltraPeers. While this may produce plentiful results, the overall affect [sic] on the network is negative as it slows queries from more reasonable clients.”<sup>199</sup> These concerns show the continuing difficulty in balancing decentralization and selfless behavior. Yet the fact that GnutellaNet remains unsued has given it an aura of continued importance in the filesharing story.

#### **D. The Legal Fate of Peer Filesharing**

---

<sup>195</sup> Kelly Truelove, *Gnutella: Alive, Well, and Changing Fast*, OpenP2P.com, Jan. 25, 2001, at <http://www.open2p.com/pub/a/p2p/2001/01/25/truelove0101.html?page=2..>

<sup>196</sup> Namely, the clients Gnute and Gnutella.it, allowed users simply to use GnutellaNet to download files. See *id.*

<sup>197</sup> *Gnutella’s Decline*, Slyck News, July 17, 2002, at <http://www.slyck.com/newsjuly2002/071702a.html>.

<sup>198</sup> *Id.*

<sup>199</sup> *Id.*

As of 2003, the story of the peer filesharing response has not ended. The final fate of the response will depend on four major, unanswered questions.

First, the technical and legal fate of Gnutella in particular is undetermined. It is apparent how mixed designs like Napster and (to a lesser extent) KaZaA have managed to reach massive scale, yet have also attracted litigation. The unanswered question is whether Gnutella or something else can scale to mass levels (tens or hundreds or millions of users) while continuing to avoid intermediary liability. The significance of Gnutella will remain minimal if it only supports a small number of users with any stability. There are reasons to view this problem as fundamental, because scaling solutions tend to require greater control over the network, increasing the odds of legal liability.

The legal status of Gnutella developers is the threshold legal question in this area. Programs like MyMP3, Napster, and now probably the FastTrack companies have been held liable based on the control they exercise over their networks. Yet Gnutella clients, like Bearshare and Limewire, are at the extreme for lacking control, even if they know that their products are predominantly used for illegal purposes. As these companies become ever closer to the status of photocopiers and VCRs, the legal question becomes harder.

It may be a surprise to hear that the law is on Gnutella's side, while copyright policy (if not social policy) favors the recording industry. Under the combined doctrine of *Sony* and *A&M Records*, the copyright owners need to either prove "actual knowledge," a proxy for network control, or a lack of commercially significant legitimate uses. The latter follows from Napster *a fortiori*, because GnutellaNet is capable of even more non-infringing uses than Napster. Meanwhile GnutellaNet's extreme lack of control would make "actual knowledge" particularly hard to prove using the *Netcom* formula of notice and failure to remove.<sup>200</sup> Gnutella, in short, was designed as if to exploit the *Napster* decision, and on paper has a good argument.

Nonetheless, courts may still not care. A court could read *Sony*, from a policy matter, as a construction of fair use to correct a perceived market failure.<sup>201</sup> While clearer as a matter of hindsight, the sense that the *Sony*

---

<sup>200</sup> See *Religious Technology Center v. Netcom Online Communications Services, Inc.*, 907 F.Supp. 1361 (1995) (announcing notice liability for service providers).

<sup>201</sup> C.f. Wendy Gordon, *Fair Use As Market Failure: A Structural And Economic Analysis Of The Betamax Case And Its Predecessors*, 82 Colum. L. Rev. 1600 (1982) (describing fair use as a mechanism for correcting market failure).

decision correctly addressed a market failure is far stronger.<sup>202</sup> It was apparent that the VCR broadened the addressable market for television shows (via time-shifting) and for movies (via rentals). Though there is an argument that file-sharing helps the music industry, it is much less intuitive than the argument that the VCR industry helped the television and movie market.<sup>203</sup> Filesharing looks more like a replacement for legitimate music sales, and therefore a straightforward erosion of the incentives of authors. This may compel a court to find some way to find Gnutella developers liable, regardless of the *Napster* precedent. The Gnutella developers, moreover, hurt their cause whenever they exercise control over their network (like requiring levels of sharing) even though the technical and social reasons for doing so are sound.

If copyright owners have trouble with Gnutella as an intermediary, will they be able to target Internet Service Providers (ISPs), like America On Line or carriers like Verizon instead? Since ISPs carry the infringing traffic, there is a natural temptation to make them responsible for ensuring that their users do not infringe copyright. Under current law, however, choosing ISPs as gatekeepers based only on their carriage of traffic is unlikely to be successful. For one thing, ISPs in their role as carriers are specifically protected against such lawsuits under §512(a) of the Digital Millennium Copyright Act (DMCA)—in the one section of copyright immunity not subject to an exception for notice and failure to remove.<sup>204</sup> Second, reflected in § 512(a), is the general understanding that placing the burden of detecting copyright infringement on neutral carriers would impose a ruinous constraint on the network.

The second unanswered question is whether programmers will continue to write ever-better or harder-to-sue peer-to-peer applications. As discussed in greater depth below, the hoped-for financial rewards of offering a filesharing application have not emerged. The potential legal liability, moreover, appears considerable. These facts could eventually end peer response as a popular, as opposed to an underground, movement. At present, however, there is no sign of abatement in the writing of new programs. Web

---

<sup>202</sup> See generally, *id.*; see also 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, 260-263 (2001) (giving the basic economic argument that Napster be held liable, author goes on to suggest Coasean complications).

<sup>203</sup> For studies supporting this position, see Chipman, *supra* note 91; Lahey, *supra* note 91.

<sup>204</sup> 17 U.S.C. §512(a) (2002).

sites like *Zeropaid* continue to make dozens of filesharing applications available.<sup>205</sup>

### E. New Enforcement Paradigms?

Copyright's beneficiaries, the content industry, reacted to P2P in the most obvious way: lawsuits. But will copyright owners be able to shift to primary enforcement to maintain similar levels of compliance? Or can they make use of technological methods themselves?

This is the sixty-four dollar question for copyright enforcement. While a full answer is beyond the scope of this Article, it is possible to look both at the record of the 1990s and at what sanction theory predicts. Everything suggests that achieving previous levels of compliance without secondary enforcement will be difficult. The future will turn on the effectiveness of using the criminal law to enforce copyright, and the effectiveness of content owner's own technological countermeasures.

The behavior of content owners themselves suggests they have little confidence in primary enforcement. Faced with the prospect of losing their gatekeeper system, content owners have spent the last decade investing in new systems of supplemental enforcement. Such investments would be expected if primary enforcement were an inexpensive alternative.

In the 1990s, for example, the industry invested considerable time and energy to ensure passage of the Digital Millennium Copyright Act (DMCA) and its anti-circumvention provisions.<sup>206</sup> Those provisions back up various technological techniques of preventing the copying of content, by criminalizing circumvention of copy protection systems. The provisions are a clear effort to maintain a gatekeeper system. Technological copy protection "respecializes" the creation and mass distribution of copyright works, while the DMCA's anti-circumvention law makes it a crime to undo the respecialization.<sup>207</sup> If successful, the effort would return owners to the easy living of the 1970s, free to sit back and police intermediaries. If

---

<sup>205</sup> Zeropaid is located at [www.zeropaid.com](http://www.zeropaid.com).

<sup>206</sup> Pub.L. No. 105-304, 112 Stat. 2860, § 103 (1998). For a description of industry efforts to have the DMCA passed, see Litman, *supra* note 97, at 122-45.

<sup>207</sup> A more recent example in the same vein is the well-known "Hollings Bill," the Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. It would require all "digital media devices" to include copy protection technology in its design. *Id.* §5(a). It can be otherwise described as an effort to place the burden of preventing copyright infringement on electronics manufacturers.

unsuccessful, digital protection will simply make legal, protected versions less attractive than illegal, unprotected competitors.

The search for a supplement also explains the funds spent trying to make people feel guilty about copyright infringement. As discussed in greater detail above,<sup>208</sup> when it comes to copying files, people have proven unaffected by the ethical tug of the copyright statute. A survey reported on by two economists showed that only 14% of respondents considered illegal copying of software to be a serious crime, compared to 30% who felt that way about driving 40mph in 25mph zone.<sup>209</sup> The software and recording industries have spent a decade trying to change that attitude. For example, a recent RIAA initiative teaches that “uploading and downloading somebody else’s music without their permission isn’t just against the law. It’s a rip-off. Simple as that.”<sup>210</sup>

Finally, content owners have invested in efforts to find new intermediaries. In the summer of 2002, the RIAA filed a lawsuit against various telephone companies who operate the backbone of the Internet, but dropped the suit a week later.<sup>211</sup> More recently, the RIAA successfully convinced a federal judge to require Verizon to identify a subscriber accused of downloading hundreds of copyrighted files in a single day.<sup>212</sup>

The extent of these efforts suggest that copyright owners do not want to resort to primary enforcement (though they have said they may be forced to).<sup>213</sup> Basic sanction theory suggests copyright owners have reason to be concerned about the limits of primary enforcement. First, unlike, for example, laws barring bank robbery, the victims of copyright infringement usually bear the costs of enforcement, including detection.<sup>214</sup> As a result, the

---

<sup>208</sup> See discussion *infra* Part 2.5.

<sup>209</sup> See Harbaugh & Khemka, *supra* note 96, at 6.

<sup>210</sup> See Soundbyting Home Page, at [http://www.soundbyting.com/html/who\\_we\\_are/are\\_index.html](http://www.soundbyting.com/html/who_we_are/are_index.html) (last visited July 24, 2002).

<sup>211</sup> Alex Pham, Tactics Toughen on Music Piracy Internet: The recording industry is seeking to block access to a foreign site and is going after individual customers of service providers, L.A. Times, Aug. 21, 2002, at C1, available at 2002 WL 2497970; Alex Pham, Technology RIAA Drops Suit Targeting Piracy Site, L.A. Times, Aug. 22, 2002, at C5, available at 2002 WL 2498191.

<sup>212</sup> *In re Verizon Internet Services*, No. Civ.A.02-MS-0323, 2003 WL 141147 (D.D.C., Jan. 21, 2003).

<sup>213</sup> See Lisa M. Bowman, File-traders in the crosshairs, CNET News, July 15, 2002, at <http://news.com.com/2100-1023-943881.html> (reporting that the recording industry is considering a program of lawsuits against end-users).

<sup>214</sup> Note that even for criminal enforcement, costs of detection have usually been borne by the owners of copyright. See *Civil and Criminal Enforcement of the Copyright Laws*:

enforcement decision is not based on the social benefits of better enforcement, but the private benefits to the copyright owner. A given class of work may be barely profitable even with full compliance with copyright, despite the fact that it has great public benefits (say, an educational work). If the private costs of enforcing the copyright against end-users outweigh the narrow profit, the result is no enforcement, even if the social calculus would dictate enforcement.

The predominantly civil nature of infringement liability is a problem for another reason: it limits the maximum sanction available, by linking it to an injunction, the value of the infringement, or statutory damages.<sup>215</sup> This is not to say that such costs, plus legal costs, would be meaningless to the average person. But on the civil side, the lack of sanctions equal to the entire wealth of the individual or the possibility of imprisonment put a ceiling on the deterrence owners can expect to achieve.

The fact that deterrence will be a collective good for all copyright owners of a given product also creates a collective action problem. It is true that copyright owners are well-organized, and have shown themselves capable of acting collectively in many contexts through organizations like the RIAA and Business Software Alliance (BSA).<sup>216</sup> Primary enforcement against home users may be different, however, because bringing suit against end-users will likely bring a considerable reputational cost for whatever entities are involved. It may lead problems of collective action to reappear.

All this suggest that the criminal side of copyright is where the question of primary enforcement will be settled. Under the little noticed and nearly unenforced No Electronic Theft (NET) Act of 1997, the government has the power to criminally prosecute even minor copyright infringement.<sup>217</sup> While this criminal statute still requires “private financial gain,” the NET Act defines “financial gain” to include “receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works.”<sup>218</sup> This makes quid pro quo file-trading potentially criminal. In the wake of the fallen gatekeeper regime, copyright owner’s copyright enforcement strategy may increasingly depend on criminal sanctions.

---

Hearing Before the Subcomm. on Patents, Copyrights and Trademarks of the Senate Comm. on the Judiciary, 99th Cong. 3, 19 (1985).

<sup>215</sup> 17 U.S.C. § 504 (2002).

<sup>216</sup> The lawsuits against Napster and other companies are examples of collective action, as are the educational campaigns discussed previously. See *supra* text accompanying notes 208-210.

<sup>217</sup> 17 U.S.C. § 101 (2002).

<sup>218</sup> *Id.*



There are signs that copyright owners will mount a major effort to convince the Justice Department to enforce the NET Act against individual peer file sharers.<sup>219</sup> On its face, the NET Act allows criminal punishment of those who violate copyright with only the expectation of receiving copyrighted works in exchange.<sup>220</sup> This amounts to an effort to increase the sanction, if not the probability of detection, for copyright infringement. Yet as pointed out in the discussion of the economic theory, there are reasons to doubt that raising sanctions will create the compliance hoped for.<sup>221</sup>

Perhaps most interestingly, content owners may take a page from the book of peer-to-peer designers, and themselves use code to influence the enforcement of copyright law, by attacking the peer-to-peer networks that undermine copyright enforcement. As a mechanism of legal influence, network design can be used both by those benefited as well as those harmed by a given law.

On June 25, 2002, Representative Howard Berman of North Hollywood, California proposed that “[t]echnological self-help” should help solve the solution to “unbridled” peer network piracy.<sup>222</sup> He proposed a bill that would give legal license for copyright owners to disrupt peer networks.<sup>223</sup> Representative Berman phrased his support of the bill, interestingly, in terms of “freedom to respond”:

[W]hile P2P technology is free to innovate new and more efficient methods of distribution that further exacerbate the piracy problem, copyright owners are not equally free to craft technological responses. This is not fair and I believe Congress should free copyright creators to develop and deploy technological tools to address P2P piracy.<sup>224</sup>

---

<sup>219</sup> See Santham Sanghera, Record industry turns fire on individual piracy, *Fin. Times Limited*, Aug. 14, 2002, at P8, available at 2002 WL 24876516 (reporting that RIAA is canvassing members to assess their willingness to pursue end-users).

<sup>220</sup> 17 U.S.C. § 506(a) (2002). The term “financial gain” was amended to “include[] receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works,” making quid pro quo file-trading potentially criminal. 17 U.S.C. § 101.

<sup>221</sup> See *supra* text accompanying notes 213-215.

<sup>222</sup> Press Release, Representative Howard Berman, Berman Announces Legislation To Foil Peer To Peer Piracy (June 25, 2002) available at <http://www.house.gov/berman/pr062502.htm>.

<sup>223</sup> To amend Title 17, United States Code, to limit the liability of copyright owners for protecting their works on peer-to-peer networks: Hearing on H.R. 5211 before the House, 107th Cong. (2002) (statement of Rep. Howard Berman).

<sup>224</sup> Press Release, *supra* note 124.

The Berman bill is extraordinary: it is the legislative license of the kind of arms-race that law is meant to eliminate. The Berman bill, while unlikely to pass, delivers support to the argument that the parties to the process consider the P2P struggle an all-out regulatory slugfest.

There are other various methods through which content owners under the Berman bill might try to disable peer-to-peer networks. One set of methods seeks to decrease the attractiveness of a peer-to-peer networks, often by flooding the network with dummy or broken music files.<sup>225</sup> Users then must spend more time looking for good files, increasing the attractiveness of conventional distribution channels. Another set of techniques would simply attack important network nodes using techniques familiar to computer hackers.<sup>226</sup> The extent to which these methods are in use today is a carefully guarded secret.<sup>227</sup> The continued activity of peer filesharing networks, however, suggests either limited success, or limited usage of such techniques.

More fanciful examples include that of a virus designed to detect illegally copied materials.<sup>228</sup> Good digital rights management is another example.<sup>229</sup> There may be a future where content owners manage to encrypt content so carefully and comprehensively from the outset, and maintain their control continuously, so that the code prevents infringement *ex ante*. Such efforts remain in their early days, and are more discussed than seen, but may eventually transform the economic dynamics of primary enforcement.<sup>230</sup> As a result, the need for gatekeepers may be eliminated, but new methods of enforcement may not need them.

The real question is not whether peer filesharing of copyrighted materials will disappear altogether—that is unlikely. The question is where the equilibrium of scale and significance is reached. Beset by new and more effective forms of regulation, peer filesharing may retreat to an underground operation, serving only a tiny subset of consumers. Alternatively, it may

---

<sup>225</sup> For an entertaining account of how anonymity can be used against peer networks, see Douglas Lichtman & David Jacobson, *Anonymity a Double-Edged Sword for Pirates Online*, *Chi. Trib.*, April 13, 2000, at 25.

<sup>226</sup> For example, a Denial of Service attack, which floods a given network node with requests until the please provide the remainder of this citation.

<sup>227</sup> See generally, Todd Woody, *The Race to Kill Kazaa*, *Wired* 11.02, Feb. 2003, at <http://www.wired.com/wired/archive/11.02/kazaa-pr.html> (surveying methods of technological self-help).

<sup>228</sup> See Michael Adler, Note, *Cyberspace, General Searches, And Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 *Yale L.J.* 1093, 1098-1100 (1996) (presenting the hypothetical of a program that roamed the net searching for contraband).

<sup>229</sup> These ideas are explored more fully in Lessig, *supra* note 144, at 177-99.

<sup>230</sup> See *id.*

grow beyond the scale of Napster, becoming the dominant means of distributing content.

#### IV

“As the largest grassroots effort in the history of the world, file trading is essentially the average person’s way of saying we don’t agree with the status quo.”<sup>231</sup>

Over the last 4 years, P2P networks have provided a sub-group of users with the equivalent of a temporary repeal for copyright for the technologically inclined. How can one explain the growth and popularity of the peer filesharing movement? I propose two answers: First, that peer filesharing uniquely suited the disorganized nature of copyright consumers as a group. Second, that P2P may represent the rational exploitation of the larger group of music consumers by a sub-set of computer savvy P2P users.

#### A. Copyright’s Divided Subjects

One reason P2P may have been successful is through the rational exploitation of “regular” consumers who lack the knowledge or resources to use P2P. In the standard (if sometimes disputed) account, copyright law is said to serve the interests of content consumers.<sup>232</sup> The law provides financial and perhaps expressive incentives to create materials that would otherwise not exist. If this is right, why would consumers ever want to disobey copyright law?

---

<sup>231</sup> Richard Menta, RIAA and MPAA sue Morpheus, Grokster and KaZaa, MP3newswire.net, at [http://www.mp3newswire.net/stories/2001/sue\\_morpheus.html](http://www.mp3newswire.net/stories/2001/sue_morpheus.html) (October 3, 2001).

<sup>232</sup> Whether copyright does indeed encourage creative expression is a question beyond the scope of this study of response. I therefore do not address the position held by some that copyright retards the creation of content. See, e.g., Eben Moglen, *Liberation Musicology*, *The Nation*, March 12, 2001, at 5; Mark Nadel, *Questioning The Economic Justification For and Thus Constitutionality of Copyright Law’s Prohibition Against Unauthorized Copying* (unpublished manuscript on file with author); cf. Stephen Breyer, *The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies, and Computer Programs*, 84 *Harv. L. Rev.* 281 (1970) (questioning whether granting copyrights in books and computer programs is really necessary to provide incentives to create and publish them).

The intuitive answer is that everyone likes getting things for free. But the answer from economic theory is more enlightening. While complying with some form of copyright law may serve the *group* interest of consumers, it is not in any given *individual's* narrow interest to comply. More generally, the logic of collective action suggests that the ideal strategy for an individual or sub-group under copyright law is to create a system that limits evasion of copyright to an “in-group,” leaving everyone else to pay for the incentives to create. To defect while others remain in compliance is to live in the game theorist’s version of utopia.

In the mid-to-late-1990s, an important demographic trend favored the development of just such a strategy. Social commentators began to use the term “digital divide.”<sup>233</sup> The term was used to refer to the fact – confirmed by empirical study – that there was a sharp division between a relatively small number of computer literate, connected citizens, and the rest of Americans. In 1998, for instance, the Clinton Administration found that college-educated Americans were almost ten times as likely to own a computer as those without any high school education (63.2% vs. 6.8%).<sup>234</sup> The disparity in internet access was even more prominent: 38.4% of college-educated Americans had access, as compared to 9.6% of those with a high school diploma, and just 1.8% of those without any high school education.<sup>235</sup>

The existence of this division in content consumers provided ideal conditions for the development of a copyright evasion strategy that could be limited to a sub-group (the technologically savvy). Peer files sharing networks were that system. By requiring at least a computer connection and internet access (and optimally broadband access and open source know-how), they guaranteed that only a certain percentage of Americans would ever be able to take full advantage of the defection from the copyright regime.

The programmers of Napster and other applications probably did not actively consider the dynamics of collective action before writing code. But users of files sharing could see that their actions could not cripple the content industry and impoverish artists. Users of peer networks were a select group that could and still do live by slightly different rules.

---

<sup>233</sup> The question of who coined the term “digital divide” remains something of a mystery. See Sharon Foster & Adrianna Borkowski, Who Coined the Term? Origin of 'Digital Divide' Escapes Even the Experts, at [http://www1.soc.american.edu/students/ij/co\\_3/digitaldivide/history.htm](http://www1.soc.american.edu/students/ij/co_3/digitaldivide/history.htm) (last visited Feb. 8, 2003).

<sup>234</sup> See National Telecommunications And Information Administration, Falling Through The Net II: New Data On The Digital Divide 4 (July 1998).

<sup>235</sup> Id.

## B. Disorganized Political Action

Even as a sub-group, however, P2P users remain disorganized. The second reason that P2P was successful was that, as an avoidance mechanism, it did not require collective action.

That content consumers have not had a strong influence on the shape of copyright law is well-documented. The lobbying process that led to the 1976 Act is a leading example. The Act was the work-product of a twenty-one yearlong negotiation between affected industry groups.<sup>236</sup> Studies suggest, however, that groups representing consumer interests had little or no influence on the shape of the 1976 Act. Jessica Litman concludes, “the citizenry’s interest in copyright and copyrighted works was too varied and complex to be amenable to interest-group championship.”<sup>237</sup>

These studies show what is obvious: for an average consumer to lobby for copyright change is expensive, likely to be futile, and, even if successful, impossible to capitalize on. As a result, very few consumers devote themselves to copyright lobbying.

Enter P2P. Individuals who participate in a peer filesharing network immediately capture for themselves the benefits of their investment. They save money on the music they download for free, with no need to share those savings with others who did not participate. Moreover, the programmers of peer filesharing programs do not even necessarily need to work together or coordinate their efforts, other than sometimes adhering to a common protocol.<sup>238</sup>

It is true that it might be difficult to convince users to *contribute*, as opposed to *take*, from the common pool of shared songs. However, the process of sharing is relatively low cost. Moreover, as Lior Strahilevitz

---

<sup>236</sup> See Litman, *supra* note 97, at 48-63 (discussing the negotiations behind the 1976 Act); see also Jessica Litman, *Copyright Legislation and Technological Change*, 68 *Or. L. Rev.* 275, 278 (1989) (same).

<sup>237</sup> Litman, *supra* note 97, at 52.

<sup>238</sup> The creation of the protocols does represent a collective action problem if they are open (that is free for anyone to develop around). Interestingly, the major open peer filesharing protocol, Gnutella, was produced by an open source programming effort. Open-source programming, motivated by technological challenges, has a proven ability to create public goods. Peter Kollock, *The economies of online cooperation: gifts and public goods in cyberspace*, in *Communities in Cyberspace* 220, 230-35 (Marc A. Smith & Peter Kollock eds., 1999) (examining the creation of the Linux operating system as an example of a public good created online despite potential collective action problems).

demonstrates, the design of P2P clients can lead users to believe that they are participating in a community, triggering norms of reciprocity.<sup>239</sup>

Does the collective action move to writing the peer application itself (the Napster program, etc.)? It does not seem to. First, provided that the program can be sold, the programmer can appropriate some of the value produced by the evasion of copyright law, and avoid the collective action problem. Second, even if it does, the investment needed to write a peer networking program may be inexpensive enough that the programmer is motivated to write if just to serve his own needs. Third, the collaborative structure of open-source software development may play a role in developing responses that rely on non-monetary incentives. I will examine each explanation in turn.

A program is a private good. If it is sold or otherwise used to generate returns, its developer has the appropriate incentive to respond on behalf of the group. This is, apparently, what has driven much of the peer filesharing response so far. For Shawn Fanning, the founder of Napster, the returns were reputational. As *Time* magazine remarked, he “reached a level of fame unprecedented for a 19-year old who is neither a sports hero nor a pop star.”<sup>240</sup> But the financial incentives for writing response programs have not proved overwhelming.<sup>241</sup> Most peer filesharing companies today depend on the dot-com model of deriving revenue from user traffic. Some developers claim that advertising revenue is enough to stay in business. For example, the developer of WinMX (yet another peer filesharing application) stated, “We stay in operation by keeping our costs low. . . . [W]e think it's smarter to skip the spyware, generate revenue from quality ad exposures on [www.winmx.com](http://www.winmx.com), and spend the money on important things such as a small yet well rewarded development team, legal contingency funds, etc.”<sup>242</sup>

More seasoned companies, however, question the advertising model. KaZaA, for example, depends on selling pop-up ads,<sup>243</sup> and plans to harness and sell the unused computing resources of its millions of peered users

---

<sup>239</sup> See Strahlievitz, *supra* note 14, at 39-53.

<sup>240</sup> Karl Taro Greenfeld, *Meet the Napster*, *Time*, Oct. 2, 2000, at 60.

<sup>241</sup> See John Borland, *Rocky financial road awaits file swappers*, *CNET News.com*, September 21, 2001, at <http://news.com.com/2102-1023-273245.html> (describing the failure of file swapping programs to make any money).

<sup>242</sup> WinMX Interview with Kevin Hearn, president, Front Code Technologies, in *Sylck News*, July 10, 2002, at <http://www.slyck.com/newsjuly2002/071002c.html>.

<sup>243</sup> See Erick Schonfeld, *The True Cost of Free Music*, *Business 2.0*, May 24, 2002, at <http://www.business2.com/articles/web/print/0,1650,40816,00.html> (describing KaZaA's business model).

(derisively referred to as a “spyware” strategy). It has freely admitted that the online advertising model does not deliver enough revenue for it to support continued development.<sup>244</sup>

Ironically, this suggests that the continuing development of peer filesharing may itself depend on copyright law’s protection. That is to say, if other revenue models prove unsuccessful, developers may have to turn to selling programs or selling membership.<sup>245</sup> Their ability to do so will depend on copyright protection, either against unauthorized distribution of the software client (perhaps using a peer network), or unauthorized circumvention of a copy-protection scheme. Peer developers may have to enlist copyright in their effort to evade copyright. They may then, in a further twist, find their tools of copyright evasion turned against them.<sup>246</sup>

Alternatively, programming a peer response may be inexpensive enough that some individuals will always be willing to undertake the project for their personal benefit alone. If a college student would otherwise spend \$500 a year on music, and if his time is not otherwise valuable, he might consider it a worthwhile investment to program an improved file-sharing application. Similarly, it could be that the challenge of peer networking development will continue to attract the collaborative attention of open-source developers. How far the open-source movement will take peer filesharing is an open question—it depends on how interesting the problem remains to programmers.<sup>247</sup>

As suggested by the change / avoidance dichotomy in Part I, one of the reasons for the success of peer-to-peer as a mechanism of legal influence is that it avoids the collective action problem inherent in change mechanisms. It has worked because certain members of the group have appropriate incentives to write programs that then lower the cost of copyright for all computer-savvy users. This fact explains the mass popularity of peer-to-peer among disorganized consumers. As a result, Napster and other programs have become an alternative to political lobbying less by choice than by default.

---

<sup>244</sup> Id.

<sup>245</sup> For example, Bearshare, available at [www.bearshare.com](http://www.bearshare.com), already sells a “professional” version.

<sup>246</sup> This is reminiscent of the fact that open source software depends on the copyright regime to enforce a license requiring that open-source code remains open. Please provide a citation for this information.

<sup>247</sup> Opinions on what motivates open-source programmers vary. See, e.g., Eben Moglen, *Anarchism Triumphant: Free Software and the Death of Copyright*, 4 *First Monday* 8, Aug. 2, 1999, at [http://www.firstmonday.dk/issues/issue4\\_8/moglen/index.html](http://www.firstmonday.dk/issues/issue4_8/moglen/index.html) (arguing that economics cannot explain why people write free software). Please provide further examples of opinions varying.

### Conclusion

It is not hard to find bold predictions for what the vibrancy of peer filesharing means for the future of governance. Reliably, John Perry Barlow's prophecies, for example, have not been understated:

What's happening with global, peer-to-peer networking is not altogether different from what happened when the American colonists realized they were poorly served by the British Crown: The colonists were obliged to cast off that power and develop an economy better suited to their new environment. . . . No law can be successfully imposed on a huge population that does not morally support it and possesses easy means for its invisible evasion.<sup>248</sup>

My own prophecies are somewhat more modest. The value of the P2P story, I want to suggest, is an understanding of how the internet has affected the ability of groups to influence law in a self-interested way. P2P has proved a useful mechanism for computer-savvy content consumers. Over the last three years, this group has enjoyed a continued reduction in the costs of the copyright system. But the mechanism is one of clear limits that become obvious on closer inspection. At best, the story suggests that groups that have never fared well in the political process, due to disorganization or unpopularity, will gain the most. Clever use of internet technologies may begin to amount to a better choice for the politically inept.

---

<sup>248</sup> See Jon Perry Barlow, *The Next Economy of Ideas*, WIRED 8.10 (October 2000).