

2003

## When Code Isn't Law

Tim Wu

*Columbia Law School*, [twu@law.columbia.edu](mailto:twu@law.columbia.edu)

Follow this and additional works at: [https://scholarship.law.columbia.edu/faculty\\_scholarship](https://scholarship.law.columbia.edu/faculty_scholarship)



Part of the [Intellectual Property Law Commons](#), and the [Science and Technology Law Commons](#)

---

### Recommended Citation

Tim Wu, *When Code Isn't Law*, VIRGINIA LAW REVIEW, VOL. 89, P. 679, 2003; UNIVERSITY OF VIRGINIA SCHOOL OF LAW PUBLIC LAW & LEGAL THEORY RESEARCH WORKING PAPER No. 03-10 (2003).

Available at: [https://scholarship.law.columbia.edu/faculty\\_scholarship/1290](https://scholarship.law.columbia.edu/faculty_scholarship/1290)

This Working Paper is brought to you for free and open access by the Faculty Publications at Scholarship Archive. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Scholarship Archive. For more information, please contact [cls2184@columbia.edu](mailto:cls2184@columbia.edu).

# UNIVERSITY OF VIRGINIA SCHOOL OF LAW

2003 SPRING PUBLIC LAW AND LEGAL THEORY RESEARCH PAPERS SERIES

## *WHEN CODE ISN'T LAW*

TIM WU

WORKING PAPER NO. 03-10

This Paper Can Be Downloaded Without Charge From The  
Social Science Research Network Electronic Paper Collection

[Http://Ssrn.Com/Abstract\\_Id=413201](http://Ssrn.Com/Abstract_Id=413201)



---



---

# VIRGINIA LAW REVIEW

---



---

VOLUME 89

JUNE 2003

NUMBER 4

## ARTICLE

### WHEN CODE ISN'T LAW

*Tim Wu\**

INTRODUCTION.....	104
I. A THEORY OF CODE, CHANGE, AND AVOIDANCE .....	110
A. <i>Reactions to Law in General Theories of Regulation</i> .....	110
B. <i>When Groups Get Sick of Complying</i> .....	112
1. <i>Avoidance Mechanisms</i> .....	112
2. <i>Change Mechanisms</i> .....	116
3. <i>Summary: The Change/Avoidance Choice</i> .....	118
C. <i>Group Dynamics, Collective Action</i> .....	120
E. <i>Avoidance, Change, and Regulatory Competition</i> .....	126
F. <i>How Code is Used to Avoid Law</i> .....	128
II. COPYRIGHT'S LOOPHOLES .....	130
A. <i>Copyright and Its Gatekeepers</i> .....	132
B. <i>The Erosion of the Gatekeeper System</i> .....	137
C. <i>Elements of Peer Design</i> .....	138
D. <i>Purity in Peer Design</i> .....	140
E. <i>Copyright and Social Norms</i> .....	143
III. THE EVOLUTION OF P2P DESIGN AND REGULATORY	
COMPETITION.....	147
A. <i>Napster and its Predecessors</i> .....	147

---

\* Tim Wu, Associate Professor of Law, University of Virginia School of Law. I am grateful to Barb Armacost, Jack Goldsmith, Scott Hemphill, Mitchell Kane, 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 and the Virginia Law School Faculty Workshop; to the Stanford Law School Internet and Society Speaker Series; and to Miriam Cho and Kelly DeMarchis for research assistance.

B. <i>Early Gnutella: 2000-2001</i> .....	151
C. <i>The KaZaA Era: 2001 - Present</i> .....	154
1. <i>FastTrack &amp; KaZaA</i> .....	154
2. <i>Next-Generation Gnutella</i> .....	156
D. <i>FastTrack and Gnutella Go to Court</i> .....	157
E. <i>The Reaction to the Reaction</i> .....	160
1. <i>Investments in Change</i> .....	160
2. <i>Extralegal Investments</i> .....	162
IV. THE SOCIAL DYNAMICS OF P2P FILESHARING .....	164
A. <i>Copyright's Divided Subjects</i> .....	165
B. <i>Disorganized Political Action</i> .....	166
CONCLUSION.....	170

#### INTRODUCTION

When the Supreme Court upheld extended copyright terms in *Eldred v. Ascroft*,<sup>1</sup> many Internet activists called for renewed political action in the form of appeals to Congress or 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 to 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” because “[t]hat’s where their competitive advantage lies.”<sup>2</sup>

The idea that computer code may be emerging as a meaningful instrument of political will remains one of the most evocative and poorly understood propositions in the study of law and technology. The prominent effects of computer code have made it difficult to ignore the fact that code can be used to produce regulatory effects similar to laws. Hence, the popularity of Professor Lawrence Lessig’s idea that (for computer users at least) “code is law.”<sup>3</sup>

But what this really means remains extremely vague. The subject remains the focus of grand speculation, ranging from claims that computer

<sup>1</sup> 123 S. Ct. 769 (2003).

<sup>2</sup> Declan McCullagh, *Geeks in government: A good idea?*, at <http://news.com.com/2010-1071-949275.html> (Aug. 12, 2002) (on file with the Virginia Law Review Association) (quoting Sonia Arrison of the Pacific Research Institute).

<sup>3</sup> See Lawrence Lessig, *Code and Other Laws of Cyberspace* 89 (1999).

code will arise as a kind of utopian sovereign to improve on perceived failures of state regulation,<sup>4</sup> to concerns that code may be used to negate basic freedoms,<sup>5</sup> and, of course, the claim that nothing of legal novelty has happened, or perhaps ever will happen.<sup>6</sup>

Most problematically, none of these understandings of code and law explains a central issue: compliance. Specifically, they do not explain the shifting patterns of legal compliance in the 2000s. Explosions of non-compliance in areas such as copyright, pornography, financial fraud, and prescription drugs fuel the sense of a legal breakdown, yet the vast majority of laws remains unaffected. The mixed compliance pattern finds little explanation in the concept that “code is law” or in notions that technological self-help can offer a substitute for legal systems.<sup>7</sup>

This Article proposes a new and concrete way to understand the relationship between code and compliance with law. I propose to study the design of code as an aspect of interest group behavior: as simply one of several mechanisms that groups use to minimize legal costs. Code design, in other words, can be usefully studied as an alternative to lobbying campaigns, tax avoidance, or any other approach that a group might use

---

<sup>4</sup> These claims are described and discussed in Timothy Wu, *When Law & the Internet First Met*, 3 *Green Bag 2d* 171, 172–73 (2000). See also 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 the efficacy of technological self-help should allow voluntary exit from the copyright regime); Kenneth W. Dam, *Self-Help in the Digital Jungle*, 28 *J. Legal Stud.* 393 (1999) (arguing that technological self-help will play a positive role in the growth of electronic commerce).

<sup>5</sup> See Lessig, *supra* note 3, at 233.

<sup>6</sup> See, e.g., Bruce P. 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); James B. Speta, *Internet Theology*, 2 *Green Bag 2d* 227 (1999) (arguing that Internet publication does not justify major changes to the First Amendment regime). One could attribute this view to Jack Goldsmith, though in his view, unfairly. See Jack L. Goldsmith, *Against Cyberanarchy*, 65 *U. Chi. L. Rev.* 1199, 1201 (1998).

<sup>7</sup> E.g., Lessig, *supra* note 3; Bell, *supra* note 4. Nor does the scholarship examining the metaphors used for Internet conduct explain compliance patterns. See, e.g., Dan Hunter, *Cyberspace as Place, and the Tragedy of the Digital Anticommons*, 90 *Cal. L. Rev.* (forthcoming 2003) (noting the persistence of the space metaphor); Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 *Geo. L.J.* (forthcoming 2003) (arguing that technological perspectives decide Internet cases); Timothy Wu, *Application-Centered Internet Analysis*, 85 *Va. L. Rev.* 1163 (1999) (arguing that analysis should focus on application development); 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).

---

---

to seek legal advantage. The approach aims to separate two different aspects of code's relationship with law. The first is Lessig's concept of a regulatory mechanism: that computer code can substitute for law or other forms of regulation. The second aspect is as an anti-regulatory mechanism: a tool to minimize the costs of law that certain groups will use to their advantage.

The code designer, I suggest, *redesigns* behavior for legal advantage. The programmer is not unlike the tax lawyer, exploiting differences between stated goals of the law, and its legal or practical limits. He targets specific weaknesses in legal regimes, and has no means to rewrite laws in general. Therefore, I argue that the long-term significance of the programmer's methods for the legal system can be described in a fairly straightforward fashion. At its greatest extent, the design of code may provide a new option for influencing specific laws. It will be of the greatest importance to individuals or large, disorganized groups poorly equipped to take advantage of existing means of political influence. And as such, the code option may mean some change in the relative power of interest groups, as it makes organization slightly less important.

The gains to diffuse groups may seem to be a positive development. But there is a darker side. Code design, as a means of avoiding laws, serves as a particularly useful device for exploiting the internal dynamics of regulated groups. It is, as this Article shows, a useful way for the computer-savvy to avoid legal burdens while continuing to enjoy the benefits of an ordered society, thanks to the continued compliance of the technophobic.

In short, increasing use of code to minimize the burden of laws has interesting and complicated effects for both the legal system and political system that have been misunderstood. The effects are categorically different from the fundamental challenge to the legal system that some had imagined, and analytically distinct from the concept that code is a form of regulation.

The important case of peer-to-peer ("P2P") filesharing, explored in depth in this Article, illustrates the possibility of using code design as an alternative mechanism of interest group behavior. 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.

P2P filesharing represents the most ambitious effort to undermine an existing legal system using computer code. The significance of P2P for

copyright is substantial. The efforts of P2P programmers have provided computer-savvy music listeners with a continuing reduction in the costs of the copyright system, comparable to a temporary repeal of copyright laws for computer geeks. P2P underlines the reality of code design as an alternative mechanism of interest group behavior.

But P2P filesharing also makes the limits of this alternative mechanism clear. The efficacy of P2P filesharing depends on two powerful and often unrecognized weaknesses of the copyright regime: the law's dependence on a gatekeeper enforcement mechanism and the severe lack of normative support among the regulated. Successful P2P networks relegate the law to an exercise in primary enforcement against a multitude of end-users.

P2P's success may depend on a unique collective action dynamic among music consumers that stems from the nature of copyrighted works. The works available on peer networks are generally non-rivalrous goods.<sup>8</sup> As a result, the sub-group of P2P users, young and computer-savvy,<sup>9</sup> can take advantage of the continued compliance of regular consumers. The mass of regular users pay for the works, thereby maintaining incentives for artists to create them, while the P2P sub-group defects *en masse*, occupying the game-theorist's version of utopia.

These weaknesses, however, represent unique problems for copyright law and are not more generalized weaknesses of the legal system. For that reason, the utility of P2P as a means of avoiding law appears limited. Only a few regimes may contain other particularized enforcement weaknesses comparable to those of the copyright regime.

This Article's claims will 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 Part I of the Article to make the underlying model clear.

Laws impose costs upon regulated groups. Those groups that seek to minimize the costs of law face a fundamental choice between mecha-

---

<sup>8</sup>That is to say, one individual's consumption does not diminish another user's value of the product. I emphasize this characteristic because some scholars 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/> (on file with the Virginia Law Review Association).

<sup>9</sup>According to an Ipsos-Reid study, those who use peer filesharing networks are predominantly between the ages of twelve and twenty-four. See Robyn Greenspan, *Making Money on Free Music*, at <http://www.internetnews.com/stats/article.php/1365161> (last visited May 12, 2003) (on file with the Virginia Law Review Association).



---

nisms of *change* and *avoidance*. Both mechanisms have the effect of lowering the expected costs of law, but the similarities end there. Mechanisms of change (principally lobbying) decrease the sanction attached to certain conduct and tend to require collective action. Mechanisms of avoidance, on the other hand, decrease the probability of detection and typically do not require that groups act collectively, but depend on specific vulnerabilities in the law.

This understanding, while not exhaustive, is descriptively useful even in the simple form presented. It clarifies the link between problems of compliance and group dynamics—the extent of organization of the regulated. It shows that changes in the costs of mechanisms of legal influence can dramatically affect the function of a given law.

Part I will conclude by explaining how the design of code can be viewed as a mechanism of legal influence. It will argue that code is used to reshape behavior to take advantage of loopholes and ambiguities in legal systems. As such, code is a mechanism of avoidance, displaying the properties of avoidance described in the model.

Part II will demonstrate the unique vulnerabilities of copyright laws and code's ability to exploit those weaknesses. Copyright enforcement has long relied on what Professor Reinier Kraakman first called a gatekeeper regime.<sup>10</sup> In other words, the copyright regime 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 presents a serious technical challenge, the goal is clear—to remove the enforcement efficiency of a gatekeeper system, leaving primary enforcement against end-users as the only option.

P2P networks also exploit an important ambiguity regarding the ethics of home copying. Compliance with laws pertaining to the theft of real property is facilitated in part by the status of clearly established norms. These norms help prevent 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>11</sup> P2P applications are designed to look

---

<sup>10</sup> Reinier H. Kraakman, Gatekeepers: The Anatomy of a Third-party Enforcement Strategy, 2 J. L. Econ. & Org. 53, 53–54 (1986).

<sup>11</sup> See Amanda Lenhart et al., The Pew Internet & Am. Life Project, Downloading Free Music: Internet music lovers don't think it's stealing 5 (Sept. 28, 2000), available at

and feel more like non-commercial home copying than like breaking into a record store. The design therefore successfully exploits the normative distinction between illegal “stealing” and innocuous “copying.”<sup>12</sup>

Part III will demonstrate how P2P protocols have grown, through several iterations, to specialize in exploiting copyright’s gatekeeper system. By its end, the P2P story suggests real limits on network design’s ability to influence law. Influencing the law in such a manner requires, particular vulnerabilities in the law and a group that lacks better options. The limits in generalizing the P2P model to other areas of law demonstrate why the compliance challenge is specific to certain classes of vulnerable laws, not a general challenge to the legal system.

Part IV will conclude by studying the fit between P2P applications and music consumers as an interest group. A fascinating aspect of the peer filesharing story is the lack of coordination and organization that characterized its development. Developers bicker and work independently, and etiquette among users must be engineered or, as Professor Lior Strahilevitz argues, induced with “charismatic code.”<sup>13</sup> Despite the chaos, peer networks have managed to provide a subset of music listeners with a continuing reduction in the costs of copyright laws.

Such results from disorganized efforts are consistent with the distinction between mechanisms of *avoidance* and of *change*. The disorganization supports the claim that matters as an option for groups whose inability to act collectively precludes better options.

Finally, the results may also reflect the current ability of P2P users to take advantage of the continued compliance of the majority of the population. The copyright regime’s subjects are divided by a technological line between the computer-savvy and regular users. Because consumption of copyrighted works is non-rivalrous, P2P users may rely on regular users to pay for music and to provide incentives for its creation, free-riding on the results.

---

<http://www.pewinternet.org/reports/toc.asp?Report=23> (on file with the Virginia Law Review Association); Office of Tech. Assessment, U.S. Cong., Copyright and Home Copying: Technology Challenges the Law 163 (Oct. 1989), at [http://www.wws.princeton.edu/~ota/disk1/1989/8910\\_n.html](http://www.wws.princeton.edu/~ota/disk1/1989/8910_n.html) (on file with the Virginia Law Review Association).

<sup>12</sup> Cf. Lior Jacob Strahilevitz, Charismatic Code, Social Norms and the Emergence of Cooperation on the File-Swapping Networks, 89 Va. L. Rev. 505 (2003) (arguing that charismatic code creates an illusion of reciprocity that accounts for why people contribute to a filesharing network).

<sup>13</sup> See generally, *id.*

---

---

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 the onset of lobbying, impact litigation, or sophisticated tax evasion, the rise of copyright evasion is best understood as a change in power dynamics among and within regulated groups.

### I. A THEORY OF CODE, CHANGE, AND AVOIDANCE

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 is a set of assumptions and arguments that Part I seeks to clarify.

#### A. *Reactions to Law in General Theories of Regulation*

John Austin, lecturing on jurisprudence in the early 1800s, sought to separate law, the “appropriate matter of jurisprudence,” from morals, religious scruples, and other distractions.<sup>14</sup> Two hundred years later, positive legal scholarship has come full circle. Rather than focusing on separating law from norms or ethics, it has pushed instead toward understanding law as part of more general theories of regulation.<sup>15</sup> Led by the law and society movement and Robert Ellickson’s book, *Order Without Law*, theorists routinely study the regulatory effects of law, group rules, social norms, and even the regulatory potential of code.<sup>16</sup> Such 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 even gave the study of law in isolation a pejorative label: “legal centralis[m].”<sup>17</sup>

---

<sup>14</sup> See John Austin, *The Province of Jurisprudence Determined* 26 (1832).

<sup>15</sup> See, e.g., Robert C. Ellickson, *Order Without Law: How Neighbors Settle Disputes* 126–32 (1991) (describing five different sources of regulation); Lessig, *supra* note 3, at 86–90 (describing four modalities of regulation: law, markets, norms, and architecture (code)). The antecedents for such general theories are in related sociological efforts. See, e.g., Donald Black, *Toward a General Theory of Social Control* xi (Donald Black ed., 1984) (collecting articles). A survey of legal scholarship in this vein can be found in Lawrence Lessig, *The New Chicago School*, 27 *J. Legal Stud.* 661 (1998).

<sup>16</sup> Lessig, *supra* note 3, at 86–90.

<sup>17</sup> Ellickson, *supra* note 15, at 4, 137–47. Oliver Williamson coined the phrase, see Oliver E. Williamson, *Credible Commitments: Using Hostages to Support Exchange*, 83 *Am. Econ. Rev.* 519, 520 (1983), although Ellickson popularized and expanded on the criticism.

Based on this work, the Internet law writers of the 1990s added the idea that the design of computer code could be understood as an alternative means of regulation, leading to the catchphrase “Code is Law.”<sup>18</sup> The idea is that programmers make choices that constrain online capability, and that such choices are regulatory in their effects. Lawrence Lessig, for example, argued that the size and weight of office buildings can be understood as a mechanism for preventing their theft, just like a law against larceny.<sup>19</sup> Similarly, he reasoned, code-based copyright protection for programs that make software difficult to steal are a form of regulation.<sup>20</sup> The same goes for code-based content-filters that might make it easier, or harder, to reach an intended audience. The design of filters is simply the code-based regulation of speech.<sup>21</sup>

But as the scope of regulatory scholarship increases, it becomes more apparent that there is something lopsided to the effort. Current scholarship pays great attention to the range of options available to regulators. But how much attention is paid to 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 necessitates understanding not only regulation options, but also 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 incomplete without incorporating the reaction to those forces. But what form will such reactions take? And how effective will they be?

Today, such questions are answered in different ways by different bodies of scholarship. In general, one answer comes from the compliance literature: 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 accounts of the behavior of the regulated by analyzing the choice between *avoidance* and *change*.

---

<sup>18</sup> See generally, Lessig, *supra* note 3.

<sup>19</sup> Lessig, *supra* note 3, at 86–90.

<sup>20</sup> *Id.*

<sup>21</sup> See generally, Lawrence Lessig, What Things Regulate Speech: CDA 2.0 vs. Filtering, 38 *Jurimetrics J.* 629 (1998).

*B. When Groups Get Sick of Complying*

What choices face an individual or group that decides to quit complying with the law and to invest in some mechanism to change its effects? This Section outlines the fundamental choice between efforts to *change* and efforts to *avoid* laws.

First, a few assumptions should be made clear. Laws and other regulations prevent groups from doing what they would otherwise want to do. As Professor 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>22</sup> A related assumption is that the initial content of laws are exogenous, the result of an unspecified political process.<sup>23</sup> As a result, groups often face laws with which they disagree and would prefer to not follow, either in individual cases or as a general matter. In this model, compliance is driven by expected costs (punishments) deriving from legal sanctions (other sources are possible, but omitted for the present).<sup>24</sup> Finally, a mechanism of legal influence is anything that, for a given price, buys a decrease in the expected punishment associated with violating a given law.

*1. Avoidance Mechanisms*

When and why do groups obey the law? Basic economic models of compliance give a very simple answer: Laws are followed when the expected costs of legal punishment exceed the expected benefits of the banned behavior.<sup>25</sup> The result is commendably simple, but, as theorists point out, only because it does not accurately describe when subjects obey the law. Two important sets of contributing factors are neglected. The first is extra-legal forces, such as social norms, that might contribute

---

<sup>22</sup> Tom R. Tyler, *Why People Obey the Law* 19–20 (1990).

<sup>23</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 72–78.

<sup>24</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). The concept of avoision is described more fully *infra* note 32.

<sup>25</sup> Albeit with much built into each side of the equation. See, e.g., Richard Posner, *Economic Analysis of Law* 242 (5th ed. 1998) ("The model can be very simple: A person commits a crime because the expected benefits of the crime to him exceed the expected costs.").

to compliance. The second is investments in mechanisms of *avoidance*, or efforts that would lower the expected costs of the law, which 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 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>26</sup> Supplemental explanations tend to rely either on normative theories or more advanced models of self-interested behavior. Some, like Professor Tyler, argue that normative considerations are central to understanding the public's decision whether to comply or not.<sup>27</sup> Others, like Professor Eric Posner, model extra-legal compliance as self-interested signaling.<sup>28</sup> Still others have modeled it as a part of self-interested models of group interaction following game-theoretic models.<sup>29</sup>

This Section, however, focuses 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

---

<sup>26</sup> See, e.g., Tyler, *supra* note 22, at 22 (“[T]he legal system cannot function if it can influence people only by manipulating rewards and costs.”); Ellickson, *supra* note 15, at 137–47 (arguing that law’s punishments only explain some of the social order we see); Eric A. 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); Paul G. Mahoney & Chris William Sanchirico, *Norms, Repeated Games, and the Role of Law* 41–48 (2002) (unpublished manuscript, on file with the Virginia Law Review Association), available at [http://papers.ssrn.com/sol3/papers.cfm?](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=311879)

[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). 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*, 10 *J. Econ. Persp.* 43 (1996) (surveying empirical work in this area); 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); 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).

<sup>27</sup> See E. Allan Lind & Tom R. Tyler, *The Social Psychology of Procedural Justice* 230–31 (1988) (developing a group value model to explain compliance); see generally, Tyler, *supra* note 22 (arguing that perception of legitimacy affects the decision to comply).

<sup>28</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 recognizing that effective signaling depends on laws being considered legitimate. See *id.* at 111.

<sup>29</sup> See, e.g., Ellickson, *supra* note 15, at 137–47 (presenting a model premised on iterated prisoner’s dilemma); Mahoney & Sanchirico, *supra* note 26 (same).

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 their classic article, *Law Enforcement, Malfeasance and Compensation of Enforcers*, Professors Gary Becker and George Stigler first argued that investments in *avoidance* should be considerations of compliance.<sup>30</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>31</sup> This insight suggests a very basic point: compliance is not simply a function of punishments, but also of the cost of mechanisms to avoid punishment.<sup>32</sup>

The compliance literature surrounding particular statutory regimes gives more particularized insight into how groups avoid laws. Avoidance of laws is a particular focus of writings on tax compliance,<sup>33</sup> and is also the subject of study in labor law,<sup>34</sup> criminal law,<sup>35</sup> environmental law,<sup>36</sup> and international law.<sup>37</sup> From these areas, a pattern emerges, indi-

---

<sup>30</sup> See Gary S. Becker & George J. Stigler, *Law Enforcement, Malfeasance and Compensation of Enforcers*, 3 *J. Legal Stud.* 1 (1974).

<sup>31</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., Mark A. Cohen & Paul H. Rubin, *Private Enforcement of Public Policy*, 3 *Yale J. on 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 and Stigler's proposal to privatize criminal law enforcement).

<sup>32</sup> This insight is described in greater depth at *infra text* accompanying notes 66–70.

<sup>33</sup> See, e.g., 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 a taxpayer's conscience via a letter had an insignificant overall impact on tax compliance); Michael J. 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 a game); Posner, *supra* note 26, at 1782 (proposing a signaling model rather than the standard state sanctioning model to explain 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 aimed at curbing tax avoidance).

<sup>34</sup> See Ronald Turner, *Reactions of the Regulated: A Federal Labor Law Example*, 17 *Lab. Law.* 479 (2002) (detailing ways in which groups practice "avoidance" of labor laws).

<sup>35</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>36</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

cating that there are two fundamentally different ways to avoid a law's sanctions. The first can be termed *evasion*. Evasion can be defined as 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>38</sup> Each, for a certain price, decreases the odds of being punished after the law is disobeyed.

There exists a second, less obvious way to avoid legal punishment. This is what Professor Leo Katz calls "avoision," which can be defined as efforts to exploit the differences between a law's goals and its self defined limits. As Professor Ronald Turner describes it, avoision represents "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>39</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 consider the taxpayer who, blocked from deducting a transfer of money to her son, devises a complicated loan scheme to achieve the same effect. Professor Leo Katz's book on avoision is full of such examples from law and other aspects of life.<sup>40</sup> One may identify a similar dynamic in Professor Neal Katyal's study of the role of substitute products in criminal deterrence.<sup>41</sup> If, for example, the goal of the drug laws is to prevent addiction and abuse, a person who opts to become an alcoholic (legal) instead of a crack addict (illegal) is practicing avoision.

These writings paint the following picture: Groups, to minimize the burdens of laws, will sometimes invest in *avoidance*. If the price is right

---

privately enforced environmental protection to traditional public statute-based regulatory schemes).

<sup>37</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 & Antonia Chayes, *The New Sovereignty: Compliance with International Regulatory Agreements* (1995) (studying compliance with treaties); Jack L. Goldsmith & Eric A. Posner, *A Theory of Customary International Law*, 66 U. Chi. L. Rev. 1113 (1999) (studying compliance with customary international law).

<sup>38</sup> Some of these are ex post examples, others are ex ante. For present purposes they are considered together.

<sup>39</sup> See Turner, *supra* note 34, at 479.

<sup>40</sup> See generally, Katz, *supra* note 24 (presenting examples of avoision).

<sup>41</sup> See generally, Katyal, *supra* note 35 (studying role of substitute products in models of criminal deterrence).



(more on this later),<sup>42</sup> they will invest in mechanisms to lower or eliminate the probability of being punished for disregarding a law. Groups may either decrease the probability of detection (as in Becker's example of a bribe) or adopt other forms of conduct with the same effects (as in Katyal's substitution effect, or Katz's avoision).

This might seem to deliver a full picture of how groups react to laws. But even at this level of generality, writings on compliance still deliver a limited picture of how individuals or groups might try to defeat a regulatory scheme. For, as the political choice literature teaches, groups also react to burdensome laws with efforts to *change* the law. The next section considers *change* mechanisms as an alternative.

## 2. Change Mechanisms

In the early 1990s, the dietary supplement industry faced a serious legal threat. Following several well-publicized deaths, the Food and Drug Administration ("FDA") proposed to regulate popular dietary supplements like other drugs, requiring proof of therapeutic value and carefully determined dosages.<sup>43</sup> The reaction of the supplement industry 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 these products.<sup>44</sup> It is by now a familiar insight from public choice theory that groups that find a law disagreeable may try to change it.<sup>45</sup> In the 1970s, a series of articles written by economists George J. Stigler and Sam Peltzman,<sup>46</sup> followed by Robert E. McCormick and Robert D. Tollison's book, *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

---

<sup>42</sup> The effect of prices of mechanisms is discussed in *infra* text accompanying notes 66–70.

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

<sup>44</sup> See 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, thereby preventing the FDA from regulating supplements as drugs or food additives.

<sup>45</sup> For a summary of work in this area, see Dennis C. Mueller, *Public Choice II* (1989), particularly chapters 13 and 16.

<sup>46</sup> See Sam Peltzman, *Toward a More General Theory of Regulation*, 19 *J.L. & Econ.* 211 (1976); George J. Stigler, *The Size of Legislatures*, 5 *J. Legal Stud.* 17 (1976); George J. Stigler, *The Theory of Economic Regulation*, 2 *Bell J. of Econ. & Mgmt. Sci.* 3 (1971) (presenting a general interest group theory of politics).

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

premise: “I begin with the presumption that what is basically at stake in regulatory processes is a transfer of wealth . . . . [B]eneficiaries [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 treats legislative change as a commodity available for purchase. Since the introduction of the model, the literature studying the specific mechanics of interest groups and lawmaking has become more sophisticated. Professor Fred McChesney, for example, proposes that law-makers are more extortionists than bribees.<sup>50</sup> He highlights lobbying’s defensive aspects (Congress threatening legislation that groups pay to avoid), and concludes that 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 with information theory, asserting that lobbying works through the selective presentation of information.<sup>52</sup> Despite these refinements, however, lobbying continues to be studied as a *change* mechanism—a tool that delivers or prevents legal change for a price.

The process of achieving legal change through litigation has also, though less often, been studied as an investment model. In Professors Landes’s and 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> Professor Jeremy Rabkin, in a 1989 work, broadly argued that, through their litigation

---

<sup>48</sup> Peltzman, *supra* note 46, at 213–14.

<sup>49</sup> William M. Landes & Richard A. 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 Stud.* 101 (1987) [hereinafter *McChesney, Rent Extraction*]; see also Fred S. McChesney, *Money for Nothing* (1997) (developing and broadening the rent extraction model) [hereinafter *McChesney, Money for Nothing*].

<sup>51</sup> McChesney, *Rent Extraction*, *supra* note 50, at 109–12.

<sup>52</sup> See, e.g., David Austen-Smith & John R. Wright, *Competitive lobbying for a legislators’ vote*, 9 *Soc. Choice & Welfare* 229 (1992) (developing a model of interest group behavior based on the notion that such lobbying is the exercise of strategic information transmission); Johan Lagerlof, *Lobbying, information and private and social welfare*, 13 *Eur. J. Pol. Econ.* 615 (1997) (same); Susanne Lohmann, *Information, access, and contributions: A signaling model of lobbying*, 85 *Pub. Choice* 267 (1995) (same).

<sup>53</sup> See Landes & Posner, *supra* note 49; Posner, *supra* note 25, at 587–90.

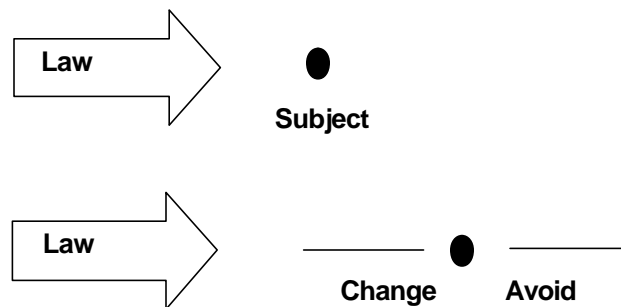
strategies, interest groups determine or radically influence the regulatory agendas of agencies.<sup>54</sup>

In a 1991 essay Einer Elhauge argued that the litigation process was equally, if not more, susceptible to interest group influence.<sup>55</sup> He argued that, generally speaking, “the same interest groups that have an organizational advantage in collecting resources to influence legislators and agencies also have an organizational advantage in collecting resources to influence the courts.”<sup>56</sup> Therefore, “[I]ncreasing the lawmaking power of the courts may only exacerbate the influence of interest groups.”<sup>57</sup> Whether Elhauge’s specific conclusion is right or wrong, he demonstrates that litigation campaigns can also be interpreted as investments in legal change.

This literature shows that mechanisms of *change* can be viewed as an alternative to mechanisms of evasion for lowering the costs of law.

### 3. Summary: The Change/Avoidance Choice

This Part has suggested that groups and individuals face a choice between avoidance and change mechanisms when deciding how to react to burdensome laws. Very simply, if a law is a cost on its subject, then *avoidance* and *change* mechanisms, the subjects of the compliance and political choice literatures respectively, can be pictured as different directions of reaction, as follows.



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

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

<sup>56</sup> *Id.* at 67–68.

<sup>57</sup> *Id.* at 68.

As identified in the discussion above, within each broader category of mechanism, are specific subcategories, such as lobbying or litigation in the case of change mechanisms, and evasion and avoidance in the case of avoidance mechanisms. Finally, while the model here focuses on law as the regulatory modality, the basic framework of analysis is meant for any source of regulation.

The following table summarizes the signal features of avoidance and change mechanisms.<sup>58</sup>

**Table 1: Change & Avoidance**

	<b>Change</b>	<b>Avoidance</b>
Types	Litigation, Lobbying	Evasion, Avoidance
Literature	Public Choice	Compliance

<sup>58</sup> Some people may feel discomfort at comparing change and avoidance in this fashion, but this discomfort may be useful and instructive. One can draw a parallel to Albert Hirschman's work on institutional feedback. See *Exit, Voice, and Loyalty*, Albert Hirschman (1970). Hirschman emphasized that members of declining institutions faced a fundamental choice between "voice" and "exit" as forms of feedback. Despite the different "feel" of voice and exit—study by different fields of scholarship, and the sense of disloyalty evident in the latter—Hirschman maintained that a useful picture of organizational feedback required understanding the choice. 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 each strategy's comparative efficiency. And if tools of avoidance are growing in sophistication, as the example of code design here studied suggests, it makes sense to understand what the consequences will be.

Nature of Good	Collective Good	Excludable Good
----------------	-----------------	-----------------

### C. Group Dynamics, Collective Action

The distinction between a group's choice of a change or avoidance strategy is 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 1964, Professor Mancur Olson made a well-known contribution to the study of interest group behavior.<sup>59</sup> Using the logic of collective action, he divided those affected by regulation into two main groups—those capable of effective political action, and the “forgotten groups” who, he argued, “suffer in silence.”<sup>60</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, making small groups and those organized for some other purpose (like unions) effective political actors and rendering large and disorganized groups essentially victims of the legislative process.<sup>61</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>62</sup>

The change/avoidance dichotomy suggests a different conclusion. Forgotten groups do not necessarily suffer in silence; instead, they *avoid* laws with which they disagree, so long as doing so is convenient. 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 does not necessarily make them inert when faced with burdensome laws. Rather, their recourse is limited to investing in avoidance mechanisms to decrease the costs of laws. One may better understand

<sup>59</sup> See Mancur Olson Jr., *The Logic of Collective Action* (1965). The logic of collective action and the problem of free-riding now underlie most present-day studies of lobbying and interest group behavior. See, e.g., Daniel A. Farber & Philip P. Frickey, *Law and Public Choice: A Critical Introduction* 17–21 (1991); McCormick & Tollison, *supra* note 47, at 17–18 (discussing organizing costs); 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>60</sup> Olson, *supra* note 59, at 165.

<sup>61</sup> *Id.* at 53–57, 132–34, 165–67.

<sup>62</sup> *Id.* at 133–67.

Olson's dichotomy between groups as an indication of who can take advantage of *change* mechanisms.

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 Eighteenth Amendment,<sup>63</sup> for example, benefited all drinkers, not just those who contributed to the effort to repeal it.<sup>64</sup> Nor was there any possibility that the repeal would be consumed or dissipated by overuse. 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 it and will subsequently free-ride on those efforts.

None of this is true of avoidance mechanisms. When a thief wears a mask to rob a bank, he is the sole and direct beneficiary of his investment. The driver using a radar detector keeps the benefits for herself. When a firm invests in a complicated tax avoidance scheme, its competitors do not benefit. In other words, investments in avoidance mechanisms create excludable, rivalrous goods. In general, avoidance mechanisms will side-step the problems of collective action inherent in change mechanisms.<sup>65</sup>

---

<sup>63</sup> See U.S. Const. Amend. XXI, § 1.

<sup>64</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* note 57, at 14 (defining public good).

<sup>65</sup> A clever observer might object that this collective/private good distinction seems to blur on further inspection. Yes, a tax avoidance scheme delivers benefits for the schemer, but if successful, it may serve as a useful model for others. A police officer, once bribed, might be easier to bribe in the future. The cars behind the driver with the radar detector might guess why she brakes suddenly. So does avoidance really present a different kind of collective action problem than investments in change?

It does, I suggest, because all of the examples posited simply represent the consumption of a private good that creates a positive externality. This distinction can be illustrated by the "popcorn/incense" example. Consider that cooking and eating popcorn will create a delicious fragrance from which others cannot be excluded. That fact does not make the popcorn itself a public good. The buyer of the popcorn reaps the reward of her investment, while also conferring a benefit on her peers. Hence, diffuse unorganized groups should be expected to eat popcorn despite the collective benefit conferred.

Replace popcorn with bribing a police officer and the same results are obtained. The briber personally reaps the benefits of the bribe in an fashion excludable and rivalrous, but she also confers a benefit on all future bribers.

Conversely, in the domain of public fragrance, the appropriate parallel to a change mechanism like lobbying is the burning of incense. It costs money to burn incense so as to produce a pleasant fragrance for the benefit of all. Hence, unlike popcorn, only organized groups will burn incense, just as only organized groups will invest in lobbying campaigns.

---

---

As a consequence it behooves third parties to sell avoidance to diffuse groups. A third party can invent a mechanism for reducing the costs of a given law, and then sell it to members of a diffuse group for profit or fame. This is what happens when drivers buy radar detectors, companies hire tax lawyers, or when music listeners download file-sharing software. A legal entrepreneur invests in creating a means of lowering the costs of law, and then sells it to groups that would otherwise comply.

A final complication with respect to avoidance and internal group dynamics is worth stating. This Part, for simplicity's sake, has modeled all laws simply as a cost to a regulated group, from which they derive no benefit. But many laws provide both benefits and costs, and this fact makes a difference for understanding the attraction of avoidance mechanisms. Avoidance mechanisms can be used to lower the cost of a given legal regime, while continuing to enjoy the benefits, through the rational exploitation of the compliance of the rest of the regulated group. The successful bank robber wants to steal money, but also wants to benefit from a healthy financial system. Tax dodgers want to avoid paying taxes while ideally enjoying public services paid for by everyone else. And, as the P2P filesharing case study explores in greater depth, getting music for free probably works best when most of the population continues to pay retail.

#### *D. Deciding to Quit*

Groups do not spend all their time avoiding laws or trying to change them; most people comply with most laws most of the time. When do individuals or groups decide to quit obeying the law and instead invest in some way to way to avoid or change it? The basic deterrence model discussed above suggests that this happens when the cost of compliance exceeds the expected cost of punishment. Theorists supplement that model by accounting for compliance stemming from costs associated with social norms and other sources. One may derive a more complete answer by introducing the option of investing in mechanisms to decrease legal<sup>66</sup> or other costs. The following discussion will show two things. First, compliance can be understood to depend less on punishment than on the cost of mechanisms of change or avoidance. Second, this discus-

---

<sup>66</sup> A caveat is necessary. 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.

sion will demonstrate the effect of a group's ability to act collectively, pooling resources to invest in legal change.

First, examine a basic case where groups obey the law when expected costs of disobedience exceed expected benefits and where there are no mechanisms to influence the law. If a traffic law mandates a fifty-five mile-per-hour speed limit, the expected benefit of ignoring the law and driving eighty miles-per-hour 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 parameters 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 = 55 mph

(2) Benefit of driving 80 mph = \$50

(3) Expected Costs = (Sanction)\*(Probability of Detection) =  $\$500 \times 0.2 = \$100$

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

the expected costs of the law. As discussed above, Becker and 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>67</sup> There are, however, a wide variety of mechanisms beyond bribes that will accomplish the same effect. For the driver, there exists a strategy of *avoidance* and one of *change*: investing in a radar detector and 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. Entities will invest in such mechanisms when the expected benefits exceed the sum of the response strategy cost and the expected costs of non-compliance (as reduced through the mechanism).

One may describe this dynamic with a very simple equation. Groups that have the option of purchasing mechanisms of legal influence will do so when:

$$\text{Expected Benefits} > (\text{Expected Costs} - \text{Mechanism Effect}) +$$

<sup>67</sup> Becker & Stigler, *supra* note 30, at 5–6.



Assume:

(4) Probability of detection = 0%

(5) Expected benefit of speeding = \$50

(6) Expected cost of radar detector = \$40

(7) Expected cost of legal punishment =  $\$500 \times 0 = 0$

$$\$50 > 0 + \$40$$

Result: Driver disregards law

### Cost of Mechanism

Apply this framework to two of the preceding 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 eighty miles-per-hour (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>68</sup>

This example demonstrates that if the mechanism of legal influence is 100% effective, like our radar detector, the expected cost of legal sanctions is reduced to zero, and thus can be eliminated from the basic investment equation. Therefore, given perfectly effective mechanisms, the only relevant inputs are the expected benefits and the cost of the response strategy, and the equation can be simplified as follows:

Investment when:

$$\text{Expected Benefit} > \text{Cost of Mechanism}$$

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

Consider a few implications of this analysis. The first example involves an avoidance strategy. If the speed limit were one hundred miles-per-hour, and hence not much of a burden, few individuals would buy the perfect \$40 radar detector. Conversely, if the speed limit were lowered to ten miles-per-hour, an onerous burden, everyone would want a

---

<sup>68</sup> Notice that for simplicity’s sake, this hypothetical has neglected the government’s response: government can, as some states do, ban the radar detector (but more on this later).

perfect radar detector, even if it cost \$500. Finally, notice that if the price of the perfect radar detector suddenly falls to \$1, it may become a worthwhile investment, even for the nearly costless one hundred mile-per-hour speed limit.<sup>69</sup>

The second example involves a lobbying campaign. Assume 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 eighty miles-per-hour is only \$50. The cost of the campaign would leave the driver \$99,950 in the red, unless he were somehow able to charge his fellow drivers for the successful repeal, an unlikely prospect.

**Compliance Given a \$100,000 Lobbying Campaign**

Assume:

- (8) Repeal makes expected costs = \$0
- (9) Expected benefit of speeding = \$50
- (10) Expected cost of campaign = \$100,000

$$\$50 < \$100,000$$

Result: Driver complies with law.

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 (a state). If the drivers organize themselves so as to divide the costs of the repeal campaign, they pay \$1 each, and such an arrangement is clearly a good deal for all involved. Stated otherwise, the cost of compliance for the group is \$50 times

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

Assume:

- (11) Repeal makes expected costs = \$0
- (12) Group expected benefit of speeding = \$5 million
- (13) Expected cost of campaign = \$100,000

$$\$5,000,000 > \$100,000$$

Result: Group repeals speeding laws.

<sup>69</sup> spo  
spe  
wh  
Stig  
“[t]  
Bed  
ally  
do,

100,000 drivers, or \$5 million. The lobbying campaign is, therefore, a bargain.

If these numbers are even close to realistic, then why are there traffic laws or any other laws that large groups find disagreeable? As already demonstrated and as basic political choice theory teaches, the answer is that groups such as drivers are not organized and have no effective mechanism to divide the costs of a campaign to change the law.<sup>70</sup> This demonstrates the conclusion urged above: Groups incapable of collective action tend toward *avoidance* mechanisms, while the organized invest in mechanisms of *change*.

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

This Article has until now focused on first-generation reactions—those of an interest group to a disagreeable law. This Section adds “reactions to the reaction” to show how regulatory competition between two opposing groups develops, with each investing in efforts to influence the law in its favor. For this analysis, the model of rent-seeking competitions is a useful descriptive, though not necessarily normative, guide.

The model has thus far treated laws exclusively as exogenously imposed costs on regulated groups. A more realistic model recognizes that the content of laws is a function of group interests, so that for every *regulated* group there exists a *beneficiary* group.<sup>71</sup> For example, if a law bans noisy sound trucks then the law regulates advertisers in the interest of town residents.<sup>72</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 investment, 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 its favor.

Just as group identity and dynamics influenced the actions of the regulated group, we should expect them to do the same for the beneficiary group. An organized, politically effective beneficiary group faced

---

<sup>70</sup> See discussion of group dynamics, *supra* text accompanying notes 59–64.

<sup>71</sup> Cf. McCormick & Tollison, *supra* note 47 (modeling groups in competition for legislative wealth transfers).

<sup>72</sup> See *Kovacs v. Cooper*, 336 U.S. 77 (1949).

with *evasion* may turn to the legislature with a request to “restore the balance.” On the other hand, diffuse beneficiaries may do little to react effectively.

Consider the following contrast. The P2P story features a subset of music consumers, in ferocious competition with the music industry, trying to avoid copyright laws. Faced with a threat to their copyright rents, the industry reacted with litigation, lobbying, and even technological countermeasures (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>73</sup> Unsurprisingly, the organization of the beneficiaries matters as much as the organization of 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. Professor Anne Krueger’s original description of rent-seeking suggested that laws create rents and that people will compete for them in various ways: “[s]ometimes, such competition is perfectly legal. In other instances, rent seeking takes other forms, such as bribery, corruption, smuggling, and black markets.”<sup>74</sup> Arguably, any group interested in changing a law to minimize its regulatory costs is engaged in a form of rent-seeking. The battle between P2P programmers and the recording industry, described in Part III, can be described as a gigantic dissipation of rents created by the monopolistic copyright system.

Groups reacting to law are acting in a self-interested fashion, and this may lead to a competition to influence the law’s effects. For several reasons, however, 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. The goals of this Part, however, are different. They are to develop a positive model describing the choices that groups face under burdensome regulation. Determining whether the reduction in rents is “worth” any particular legal regime is beyond this Part’s scope.

---

<sup>73</sup> On the contrary, Congress passed the Internet Tax Freedom Act, 47 U.S.C. 1151 (1998), restricting the power of states to tax Internet-based commerce .

<sup>74</sup> Anne O. Krueger, *The Political Economy of the Rent-Seeking Society*, 64 *Am. Econ. Rev.* 291, 291 (1974).

In addition, the interests of the rent-seeking literature are different than those of this Article. What makes a tool interesting to the rent-seeking literature is its potential for generating waste and the existence or absence of any socially valuable byproduct. Hence, what scholars study for rent-dissipating effects can range from research and development (rent dissipation in pursuit of patent follow-ons)<sup>75</sup> to follow-on creation in copyright<sup>76</sup> to efforts to monopolize.<sup>77</sup> It is nonetheless extremely difficult to evaluate whether alternative mechanisms of undermining legal systems have less or more valuable byproducts.<sup>78</sup> Is investing in a tax shelter more or less socially wasteful than lobbying? Such questions seem nearly impossible to answer. What this Part examines is not the relative wastefulness of mechanisms used to influence law, but their relative cost and relationship to group dynamics.

#### F. How Code is Used to Avoid Law

The premise of this Article is that “law-busting” code should be studied as a mechanism of legal influence. That is to say, it can usefully be studied alongside litigation, lobbying, tax avoidance, and other ways groups seek to influence the law in their favor. This final Section asks: how exactly does code influence the effects of law? And how does it fit within the avoidance/change dichotomy just described?

The hint of an answer comes from existing work that tries to understand the role code plays in the legal environment.<sup>79</sup> In *Code and Other*

---

<sup>75</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>76</sup> See generally, Michael Abramowicz, *Copyright Redundancy* (Geo. Mason L. & Econ. Research Paper No. 03-03, 2003), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=374580](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=374580) (on file with the Virginia Law Review Association) (arguing that copyright laws prevent wasteful redundancy).

<sup>77</sup> See e.g., Richard Posner, *The Social Costs of Monopoly*, 83 J. Pol. Econ. 807 (1975) (modeling and estimating social costs of monopoly and monopoly-inducing regulation in the U.S.).

<sup>78</sup> See *id.* at 811 (analyzing assumption that expenditures on monopolizing have no socially beneficial byproduct).

<sup>79</sup> A common question is this: Is there any particular significance to code in this regard, as opposed to just advances in technology and their effects on compliance? The argument for a special relevance for code relies on the idea that computer code has achieved a greater granularity than the technologies that preceded it: Programmers can very precisely shape behavior using code to match the particularized loopholes in laws. At previous levels of technology, conversely, such questions would arise less frequently.

---

*Laws of Cyberspace*, Professor Lawrence Lessig writes that “[i]n cyberspace we must understand how code regulates . . . . *Code is law.*”<sup>80</sup> Similarly, writers like Professors Tom Bell or Kenneth Dam, interested in “technological self-help,” are primarily concerned with the use of code as a substitute for contract, copyright, or other legal systems.<sup>81</sup>

Even though this work is interested in code “as law,” its depiction of how code achieves regulatory effects is useful. The idea is that code regulates by directly constraining behavior. Lessig argues that code “constitute[s] a set of constraints on how you behave;”<sup>82</sup> it “constrains some behavior by making other behavior possible, or impossible.”<sup>83</sup> Just as a brick wall built in the middle of the road modifies behavior, code regulates by specifying, in advance, what behavior is and is not possible. Similarly, I propose that code can influence the effects of law by *re-designing* behavior for legal advantage. That is to say, the reason that code matters for law at all is its capability to define behavior on a mass scale. This capability can mean constraints on behavior, in which case code regulates, but it can also mean shaping behavior into legally advantageous forms.

In this view, the code designer acts like a tax lawyer. He looks for loopholes or ambiguities in the operation of law (or, sometimes, ethics). More precisely, he looks for places where the stated goals of the law are different than its self-defined or practical limits. The designer then re-designs behavior to exploit the legal weakness.

Code design, as we have seen it, is a mechanism of *avoidance* rather than a mechanism of *change*. Nothing the code designer does rewrites laws. Instead, code design defines behavior to avoid legal sanctions. This description of how code “works” to influence law’s effects, I suggest, fits most of the major efforts to use code for legal advantage. Consider four examples:

*Virtual Child Pornography.* Congress passes a law banning child pornography, citing a compelling interest in preventing harm to children. Programmers create child pornography that involve no children in its

---

<sup>80</sup> Lessig, *supra* note 3, at 89.

<sup>81</sup> See Bell, *supra* note 4 (model of technological self-help); Dam, *supra* note 4 (same).

<sup>82</sup> Lessig, *supra* note 3, at 6, 89.

<sup>83</sup> *Id.*

production. The behavior has been reshaped to adapt to the limit on government's power in the First Amendment.<sup>84</sup>

*Overseas Gambling.* Laws banning gambling are territorial in jurisdiction. Casinos place their servers overseas. The conduct of gambling has been reshaped to avoid the law's self-defined jurisdictional limits.

*Junk Email.* Unsolicited advertising by mail and fax are regulated by laws specific to the mail system and fax machine, respectively. Advertisers design programs to transmit electronic mail and pop-up advertisements. The use of junk email gives advertisers an unregulated partial substitute for the mail or fax machines.

*P2P Filesharing.* The legality and ethics of "home copying" are somewhat ambiguous, and copyright has no record of enforcement against end-users. Designers build software that shapes the mass distribution of copyrighted works into a form resembling home copying.

None of this, of course, is a comment on whether these strategies will be successful in the long term. Each, as previous sections suggest, may incur a reaction to the reaction—an effort to change the law to "restore the balance." But it is clear from these examples how code design achieves its effects.

This basic theory of mechanisms underlies the claims in the rest of the Article. Part II examines the important example of P2P filesharing to show how, in practice, the design of code influences the effects of law.

## II. COPYRIGHT'S LOOPHOLES

On December 8, 1999, a group of eighteen record companies announced that they had sued a small startup company for copyright infringement.<sup>85</sup> The Recording Industry Association of America ("RIAA") forecast that it could do 100 million dollars in damage to sales,<sup>86</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>87</sup>

---

<sup>84</sup> Cf. *Ashcroft v. Free Speech Coalition*, 122 S. Ct. 1389 (2002) (striking down ban on computer-generated child pornography).

<sup>85</sup> See Don Clark, *Recording Industry Group Sues Napster, Alleging Copyright Infringement on Net*, Wall St. J., Dec. 9, 1999, at B18.

<sup>86</sup> *Id.*

<sup>87</sup> Lauren Goldstein, *Tune In: MP3 goes mainstream, but Internet music has yet to find its perfect form*, *Tune In*, *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 like a “bazaar,” alleged the plaintiffs,<sup>88</sup> but one where the goods were all 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.<sup>89</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>90</sup> Napster responded that it simply provided a “listing service.”<sup>91</sup>

If not as ruinous as the recording industry suggested it would be,<sup>92</sup> Napster emerged as a powerful force in the distribution of music. At its height, Napster claimed sixty million registered users and as many as twenty-six million active ones.<sup>93</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>94</sup> The economic effects of Napster on the music industry were, naturally, disputed in litigation.<sup>95</sup> According to some figures, global music sales tumbled

---

<sup>88</sup> Complaint at 2, *A & M Records v. Napster, Inc.*, 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) (on file with the Virginia Law Review Association) [hereinafter *Complaint*].

<sup>89</sup> See Damien A. Riehl, *Peer-to-Peer Distribution Systems: Will Napster, Gnutella and Freenet Create a Copyright Nirvana or Gehenna?*, 27 *Wm. Mitchell L. Rev.* 1761, 1768 (2001).

<sup>90</sup> *Complaint*, supra note 88, at 2.

<sup>91</sup> Clark, supra note 85.

<sup>92</sup> See *Complaint*, supra note 88, at 3 (alleging that “Napster’s conduct has caused and continues to cause plaintiffs grave and irreparable harm”).

<sup>93</sup> The estimates of Napster’s use vary. See, e.g., Jon Healey, *Napster CEO Pitching a New Tune to Labels*, *L.A. Times*, Nov. 25, 2001, at C5 (reporting sixty million active users at Napster’s peak); *Napster Use Slumps 65%*, *BBC News*, at <http://news.bbc.co.uk/2/hi/business/1449127.stm> (July 20, 2001) (on file with the Virginia Law Review Association) (reporting statistics from Jupiter Media Metrix stating that Napster had 26.4 million active users in February 2001 before the numbers began to decline).

<sup>94</sup> See Geoff Nicholson, *Will the RIAA pass up Napster’s \$1 billion offer?*, at <http://www.hitsquad.com/smm/news/708/> (Feb. 21, 2001) (on file with the Virginia Law Review Association).

<sup>95</sup> See *A & M Records v. Napster, Inc.*, 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 14–15* (Cato Policy Analysis No. 438 May 15, 2002), available at <http://www.cato.org/pubs/pas/pa438.pdf> (on file with the Virginia Law Review Association).



nearly half a billion dollars in 2000.<sup>96</sup> Sales of CD singles (the clearest Napster competitor) declined nearly forty percent that year.<sup>97</sup> In contrast, other studies suggested that Napster actually led its users to buy more CDs.<sup>98</sup>

How did any of this happen? How did a simple program have such a powerful effect on 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, relative to other sets of laws, proved so vulnerable to code-based attack. What is it about the enforcement structure of the copyright system that made it so easy to defeat? And does it share characteristics with other legal enforcement systems?

This Part argues that the success of P2P depends 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 and unusual lack of normative support among the regulated.

These weaknesses suggest several conclusions about the nature of P2P and code design as mechanisms of avoidance. P2P, in particular, probably implicates the specific weaknesses of the copyright system more than it implicates vulnerabilities in other sets of legal rules. As a general rule, code design will depend on identifiable weaknesses in legal enforcement.

#### A. Copyright and Its Gatekeepers

Common intuition dictates that laws can be vulnerable to mass disobedience, whether at rock concerts or during tax time. These problems stem from the limits and costs of "primary" enforcement (enforcement against individual violators). The costs of raising punishments increase while the benefits exhibit diminishing returns. Theorists explain these limits as stemming from administrative and third party costs, the limited

---

<sup>96</sup> Patrick Brethour, Music sales tumble 1.3% worldwide, *The Globe and Mail* (Boston), Apr. 20, 2001, at B1.

<sup>97</sup> Jeff Leeds, Record Industry Says Napster Hurt Sales, *L.A. Times*, Feb. 24, 2001, at C1.

<sup>98</sup> See *Napster*, 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, available at <http://www.itworldcanada.com/portals/portalDisplay.cfm?oid=E19EF5FC-8783-45AE-AB14E3C8BA85856F> (on file with the Virginia Law Review Association).

net worth of defendants, the lack of any punishment beyond the death penalty, and even the constitutional prohibition on cruel and unusual punishments.<sup>99</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>100</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>101</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 law’s long dependence on a gatekeeping regime is under-recognized.<sup>102</sup> The copyright law regulates a large and disparate group of content consumers, such as music listeners and book readers. The solu-

---

<sup>99</sup> These reasons are summarized in Posner, *supra* note 25, at 243–50; Kraakman, *supra* note 10, at 56–57. See also Katyal, *supra* note 35, at 2414–15 (“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>100</sup> Kraakman, *supra* note 10, at 53.

<sup>101</sup> In his influential 1986 article, Kraakman demonstrated that “gatekeeper liability” could 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) (arguing that analysis of reputational intermediaries remains incomplete without consideration of a variety of additional factors); Luigi Alberto Franzoni, *Independent Auditors as Fiscal Gatekeepers*, 18 *Int’l Rev. L. & Econ.* 365, 365 (1998) (analyzing gatekeeper regimes in tax enforcement); Ronald J. Gilson, *The Devolution of the Legal Profession: A Demand Side Perspective*, 49 *Md. L. Rev.* 869, 883–84 (1990) (analyzing the gatekeeper role lawyers play in avoiding strategic litigation); Frank Partnoy, *Barbarians At The Gatekeepers?: A Proposal For A Modified Strict Liability Regime*, 79 *Wash. U. L.Q.* 491, 491–93 (2001) (arguing for a strict liability gatekeeper regime for securities fraud). None, however, considers a statute’s dependence on gatekeeper liability to be a potential weakness.

<sup>102</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), available at <http://econ.mckenna.edu/papers/2000-14.pdf> (on file with the Virginia Law Review Association). 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.

tion to mass disobedience in this area has involved one such gatekeeper regime. That is, copyright law 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; later gatekeepers included record manufacturers, film studios, and others who produced works on a mass scale. Their role resembled that of 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>103</sup>—it could not be otherwise after the United States Supreme Court's decision in *Sony Corp. of America v. Universal City Studios*.<sup>104</sup> 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>105</sup>

There is evidence to suggest that copyright was in fact entirely dependent on gatekeeper enforcement until quite recently. Unfortunately, academic study of copyright enforcement is sparse.<sup>106</sup> What we can learn about enforcement patterns comes largely from the few hearings and

---

<sup>103</sup> See, e.g., Jessica Litman, *Digital Copyright* 111 (2001) (“Our copyright laws have, until now, focused primarily on the relationships among those who write works of authorship and disseminate those works to the public.”); 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).

<sup>104</sup> 464 U.S. 417 (1984). In the Sony litigation, the broadcasting industry targeted Sony and its new Betamax videotape 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>105</sup> Ginsburg, *supra* note 103, at 1488.

<sup>106</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 Sri-kantiah, *The Response of Copyright to the Enforcement Strain of Inexpensive Copying Technology*, 71 *N.Y.U. L. Rev.* 1634, 1643–45 (1996).

congressional studies on copyright enforcement and the case record itself.

Reflecting an interest in bigger targets, copyright laws reflected 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>107</sup> Congress described the practice of non-commercial home recordings as “common and unrestrained.”<sup>108</sup> In the 1973 photocopying case *Williams & Wilkins Co. v. United States*, the United States Court of Claims similarly stated, “[I]t 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>109</sup>

Even in the 1976 Copyright Act, Congress made the decision to limit the exclusive right of performance of audiovisual works to public performances, thereby excluding private or home performances.<sup>110</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>111</sup> The law’s indifference toward home copying was evident in the obvious 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>112</sup> Beyond this limited example, individualized infringement actions were absent until the 1990s.<sup>113</sup>

---

<sup>107</sup> H.R. Rep. No. 92-487, at 7 (1971).

<sup>108</sup> *Id.*

<sup>109</sup> 487 F.2d 1345, 1350 (Ct. Cl. 1973), *aff’d* by an equally divided Court, 420 U.S. 376 (1975).

<sup>110</sup> 17 U.S.C. § 106(4) (2000).

<sup>111</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>112</sup> *Universal City Studios v. Sony Corp. of Am.*, 480 F. Supp. 429, 432 (C.D. Cal. 1979); see also *Sony*, 464 U.S. at 434 (“The two respondents in this case do not seek relief against the Betamax users who have allegedly infringed their copyrights.”).

<sup>113</sup> The 1990s saw an effort by software copyright owners to enforce copyrights against end-users, who tend to be fairly large entities. See, e.g., Elizabeth Hurt, *Software Pirates*

The Supreme Court's decision in *Dowling v. United States* and others like it come closest to primary enforcement against individuals.<sup>114</sup> *Dowling* featured two Elvis enthusiasts who pressed unreleased recordings without permission—so-called “bootleggers.”<sup>115</sup> But these bootleggers actually created sizable distribution channels. The two hobbyists grew to do “substantial business,”<sup>116</sup> eventually functioning just like regular record-sellers themselves. They printed catalogs and advertisements, and they sold and distributed thousands of albums.<sup>117</sup> Were these Elvis bootleggers gatekeepers in the enforcement sense? They were, in the sense 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>118</sup> As the Congressional Office of Technology Assessment stated in its 1989 report, “All 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>119</sup> This report, echoed by hearings on copyright enforcement in the 1980s, confirmed that the existing pattern of enforcement by the RIAA and the motion picture industry targeted large-scale commercial pirates.<sup>120</sup> After clarifying copyright's long reliance on a gatekeeper system, one may

---

Sued: Alleged culprits targeted online auction bidders, *Business 2.0*, (Jan. 26, 2001), at <http://www.business2.com/articles/web/print/0,1650,16147,00.html> (on file with the Virginia Law Review Association). For an argument that such enforcement actually creates more piracy, see Harbaugh & Khemka, *supra* note 102, at 2.

<sup>114</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) (enforcing against a bootlegging enterprise), and *Paramount Pictures Corp. v. Labus*, No. 89-C-797-C, 1990 U.S. Dist. LEXIS 11754 (W.D. Wis. Mar. 23, 1990) (involving the operator of a small resort sued for renting pirated movies to his customers).

<sup>115</sup> 473 U.S. at 210–11.

<sup>116</sup> *Id.* at 212.

<sup>117</sup> *Id.* at 211–12.

<sup>118</sup> The Office of Technology Assessment noted that the proportion of people who made home audiotapes doubled in the 1980s. Office of Tech. Assessment, *supra* note 11, at iii.

<sup>119</sup> *Id.* at 7.

<sup>120</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 Donald C. Curran, Acting Register of Copyrights) (“RIAA is selective in what they refer to Justice, turning over only the most egregious cases.”).

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

### *B. The Erosion of the Gatekeeper System*

Gatekeeper regimes have an obvious weakness: They depend on a 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. As demonstrated by *Dowling*, there could and did arise corruptible publishers who would produce illicit copies (just as corruptible doctors hand out illicit drugs), but so long as the costs of finding such corrupted intermediaries remained reasonable, gatekeeper liability continued to prevent copyright infringement.

The erosion of copyright's gatekeeper system is an ongoing and incomplete process. The erosion proceeded in several steps, culminating in the advanced versions of P2P filesharing networks evident today.

Digitalization—the ability to make perfect digital copies of content—was the beginning of a real problem for the gatekeeper regime. It made copying certain forms of content possible for 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>121</sup> By the 1990s, an 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 the gatekeeper system: It simply 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 remained identifiable and easy to sue—retail outlets, publishers, and so on—the gatekeeper regime could remain effective.

Hence, the mass popularity of the Internet in the mid-1990s was another step toward the erosion of the gatekeeper system. But it is also a mistake to confuse the potential of the Internet as a mass dissemination system with the development of an application for such purposes.<sup>122</sup>

---

<sup>121</sup> See Office of Tech. Assessment, *supra* note 11, at iii.

<sup>122</sup> See generally, Wu, *supra* note 7 (pointing out that the Internet and its applications should be understood separately for legal analysis).

---

---

Web-based Internet outlets—say, online retailers like Amazon.com—were and are no less amenable to being copyright gatekeepers. However, it took the design of P2P filesharing systems to realize the full extent of the network's structural challenge to a gatekeeper liability system.

A pure P2P design is the logical corollary to a gatekeeper enforcement system. The design goal of a pure P2P network is the complete elimination of intermediaries. Such a pure P2P network is a network of perfect equals, each of which is both a consumer and a distributor of copyrighted materials. Such a network would force those who enforce copyrights to rely exclusively on primary enforcement, with its attendant difficulties.

Today's successful P2P filesharing applications approach, but do not achieve, a pure P2P model. The following Section explains why.

### *C. Elements of Peer Design*

The design of P2P applications to avoid copyright presents a technical challenge with implications not fully appreciated by legal scholarship.<sup>123</sup> The technical study of P2P design shows that designing a P2P filesharing network to avoid copyright requires important deviations from the optimal design for speed, control, and usability. The programmers of a copyright-resistant P2P network must balance an interest in avoiding legal liability against the competing interests of ensuring performance on a mass scale, maintaining system stability, and fostering network trust. These matters all require control over the network, while a pure peer design eliminates control as much as possible.

The goals of peer filesharing applications are a good place to begin the discussion. Two people can trade files easily, using e-mail or a floppy disk, but what about one million people? The general goal of a P2P 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 regular home users can download—a program that, running on their computers, can locate other users, creating a network of peers. Second, it requires a way for each user to search the network (or parts of it) to determine what

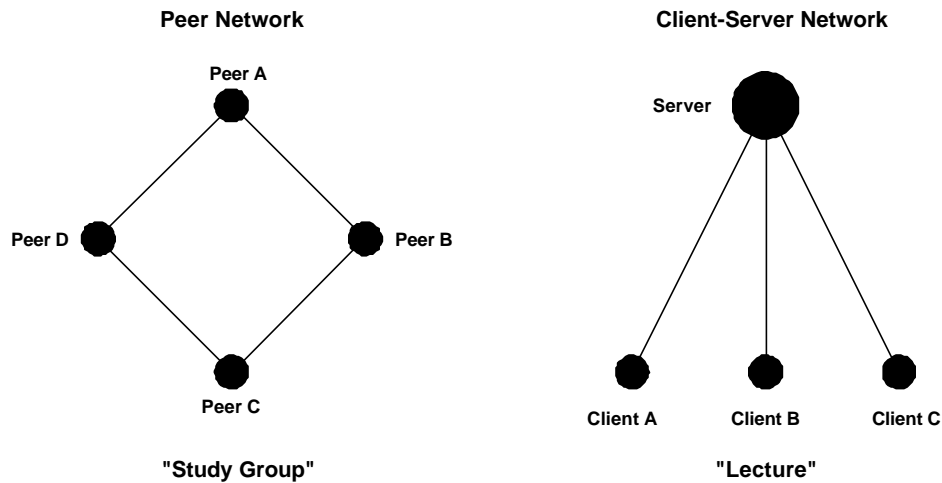
---

<sup>123</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 203, 205–06 (Andy Oram ed., 2001).

content others are making available. Third, it requires a way for users to send files to each other once they have found something desirable.

Designers accomplish these filesharing goals using a P2P design. Formally, a P2P network is an application architecture where each “node,” or computer, has equivalent rights and responsibilities.<sup>124</sup>

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



This design, as the name suggests, makes a P2P network one of equals, or peers. This network architecture should, usually, be distinguished from a “client-server” network in which one computer (the server) specializes in serving the needs of others (the clients).

Real-world metaphors help capture this important distinction. Consider the difference between a study group comprised entirely of students and a lecture led by 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. On the other hand, the classroom is a “client-server” 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.

<sup>124</sup> See Michael A. Gallo & William A. Hancock, *Networking Explained* 11 (1999).



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. Purity in Peer Design*

The distinction between peer and client-server designs is critical to understanding the challenge of building a network that resists copyright enforcement. The closer a network comes to a pure P2P design, the more disparate the targets for copyright infringement and the greater the threat to a gatekeeper system.

Why not always build the most decentralized design possible? The general answer is that 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>125</sup>

Pure peer networks are a design challenge because eliminating intermediaries decreases control over the network. The loss of control makes it difficult to ensure performance on a mass scale, to establish network trust, and even to perform simple tasks like keeping statistics. As networks grow, these problems become more pronounced. It is simple, in other words, to build a pure P2P network for six friends interested in trading, just as it is simple to maintain a study group with six members. It is difficult, however, to make the same design work for ten million people.

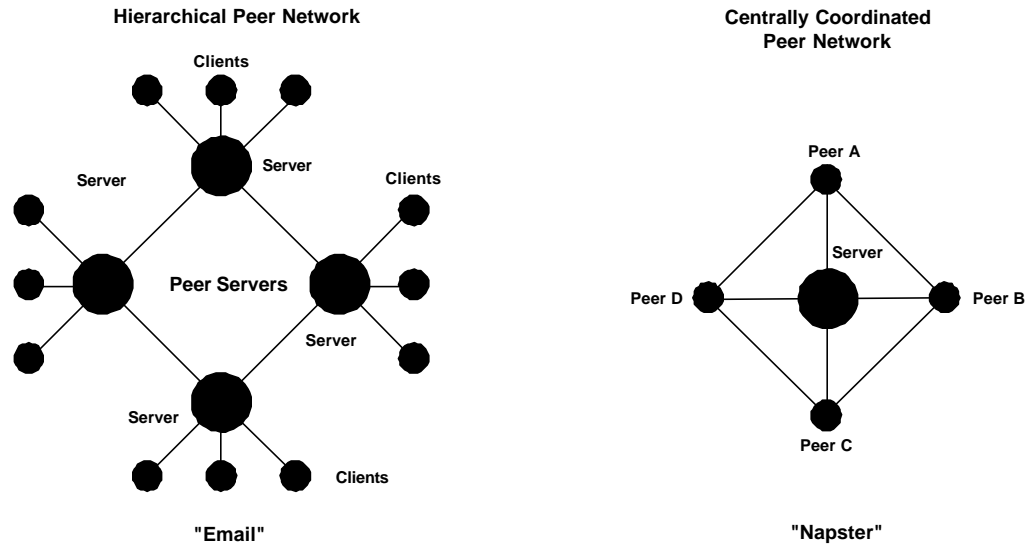
In practice, there are four recognized classes of application design. They are pictured in Figures 1 and 2 and are summarized in Table 2. Figure 1 depicts the two extremes. The Internet’s most important application, the World Wide Web, represents an archetypal client-server model. “Pure” peer design, meanwhile, is what the early version of the Gnutella peer filesharing programs adopted to avoid infringement liability.

---

<sup>125</sup> See, e.g., Gene Kan, Gnutella, *in* *Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology*, supra note 123, at 94, 117 (“the debate . . . burning in the technology community . . . [is] what is truly peer-to-peer.”); Clay Shirky, What is P2P . . . And What Isn’t?, *The O’Reilly Networks*, at <http://www.oreillynet.com/pub/a/p2p/2000/11/24/shirky1-whatisp2p.html> (Nov. 24, 2000) (on file with the Virginia Law Review Association) (arguing that the label describing what is happening to networks, “peer-to-peer,” does not clarify much).

It is often useful in a peer design to have at least one central server in which to store user information, search databases, and create a system of trust. 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>126</sup>

**Figure 2: Hybrid Designs**



To complete the classification, many of the most well-known networks are hybrids that balance control and decentralization. They appear to be P2P networks to the end-users but they are actually only P2P between specialized servers. This “hierarchical peer-to-peer” network, pictured on the left of Figure 2, supports regular Internet Protocol (“IP”) e-mail, the Domain Name System (DNS), and the classic newsreader “USENET.”<sup>127</sup> With e-mail, no central authority controls delivery of

<sup>126</sup> See Nelson Minar et al., A Network of Peers: Peer-to-Peer Models Through the History of the Internet, in *Peer-to-Peer: Harnessing the benefits of a Disruptive Technology*, supra note 123, at 3, 17.

<sup>127</sup> See M. Horton & R. Adams, The Internet Eng’g Task Force, Standard for Interchange of USENET Messages, at <http://www.ietf.org/rfc/rfc1036.txt> (1987) (on file with the Virginia Law Review Association) (detailing structure of USENET system).

messages. Rather, a particular university's or company's servers communicate with other institutional servers in a P2P fashion.<sup>128</sup>

**Table 2: 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

As this discussion shows, what is called a peer network may be decentralized in only certain respects. Examining the life cycle of a node in a peer network shows how often intermediaries are needed to smooth the functioning of even the most basic network. Of course, every intermediary becomes a potential legal target.

To begin life as a peer node, a user needs to install the appropriate software. This usually means downloading it from an intermediary (typically a web site). The node must find at least one peer to join the peer network, but how can this location be done without knowing a peer in advance? Again, the solution is usually reliance on some intermediary, such as a "host cache," that grants the peer node one peer address so that the user may begin to use the network.

To be useful, the peer node must have some ability to discover what content is available on the network. For example, in a network meant to

<sup>128</sup> See P. Mockapetris, The Internet Eng'g Task Force, Domain Names—Implementation and Specification, at <http://www.ietf.org/rfc/rfc1035.txt> (1987) (on file with the Virginia Law Review Association) (detailing design of domain name system).

---

---

share music, a user needs to know what songs are actually available, preferably by searching by artist, song title, etc. The very volume of search traffic thus generated, however, can strain a network design to the point of collapse.<sup>129</sup> Designers may minimize this effect if they design the network to access a finite amount of content (for example, hit songs). Nonetheless, designing a network remains a fundamental challenge. It is easiest to store search information in one place, but if search information is centralized, as it is in the Napster design, it creates yet another specialized intermediary.

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.” Trust systems are difficult, if not impossible, to create without some centralized system of verification.

The preceding description is a summary of the challenges facing P2P technology. The point is that P2P design represents a serious challenge for designers because it requires compromise. Fewer intermediaries means fewer targets for an infringement lawsuit. The existence of fewer intermediaries, however, makes it harder for users to use the system, creates a greater risk of system crashes, and increases the risk of anonymous attacks. There is a tension between an optimal P2P filesharing network and the goal of avoiding copyright liability. This condition will bear strongly in the examination of P2P programming incentives. The next Section considers how P2P designs have sidestepped social norms that might have prevented copyright infringement.

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

According to a 2000 Pew Internet Project study, seventy-eight percent of those who download music do not consider it to be stealing and sixty-one percent do not care if the music they download is copyrighted.<sup>130</sup> A survey reported by two economists showed that only fourteen percent of respondents considered illegal copying of software to be a serious crime, compared to thirty percent who felt that way about driving forty miles per hour in a twenty-five miles-per-hour zone.<sup>131</sup> These statistics suggest

---

<sup>129</sup> See Kan, *supra* note 125, at 112–14.

<sup>130</sup> See Lenhart et al., *supra* note 11, at 5.

<sup>131</sup> See Harbaugh & Khemka, *supra* note 102, at 6.

that P2P applications have not only undermined copyright's gatekeeper regime, but have also successfully sidestepped social norms that might otherwise bolster compliance with the copyright regime. This Section describes how code designers structured their applications to avoid social norms.

As discussed above, theorists have suggested that the possibility of state punishment provides an incomplete explanation for observed compliance with societal rules.<sup>132</sup> Rather, they suggest that other systems of social control, including social norms, account for compliance.<sup>133</sup> While accounts differ, the arguments contend that some mix of the threat of external social sanctions,<sup>134</sup> the fear of sending the wrong signals to others,<sup>135</sup> and the internalization of ethics<sup>136</sup> creates compliance that exceeds what would be observed as a simple reaction to the threat of punishment.

Those who benefit from copyright laws benefit from the norm 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. Despite their cosmetic differences, economically speaking, each instance of copying represents approximately the same economic loss in the form of a lost potential sale.<sup>137</sup>

Therefore, the system of social norms, like the gatekeeper regime, is an alternative mechanism for creating compliance with a given legal rule. If norms track the substance of legal rules, it stands to reason that a rational, widespread effort to reduce the costs of regulation may sidestep the enforcement of legal rules by manipulating social norms. If it were considered disgraceful to download music on the Internet, copyright compliance could be achieved without active, primary enforcement. The design of P2P networks, however, successfully exploits the status of

---

<sup>132</sup> See *supra* note 26 and accompanying text.

<sup>133</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 26, at 41–48 (suggesting that the state's punishments play a role in sustaining strategies of cooperation with legal rules).

<sup>134</sup> A classic external sanction model is provided in Ellickson, *supra* note 15, at 124–26.

<sup>135</sup> The signaling theory is presented in Eric A. Posner, Symbols, Signals, and Social Norms in Politics and the Law, 27 *J. Legal Stud.* 765, 766–67 (1998).

<sup>136</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) (characterizing internalization as the precondition of a norm's existence).

<sup>137</sup> Assuming a similar likelihood that the thief or friend would have otherwise paid the full price for the music.

copyright norms, 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 conducted a 1989 survey regarding attitudes toward home copying.<sup>138</sup> The study found a simple norm: people think copying for friends is okay, but copying for money is wrong.<sup>139</sup> More precisely, it found that large majorities (sixty-three percent) of consumers considered making a taped copy of audio materials for a friend to be “acceptable” or “perfectly acceptable.”<sup>140</sup> On the other hand, the greater majority (seventy-six percent) found selling copied materials unacceptable.<sup>141</sup> The survey mirrors widespread anecdotal evidence<sup>142</sup> suggesting a normative difference between commercial and non-commercial copying.

P2P filesharing exploits this distinction brilliantly. P2P clients create no sensation or impression of stealing (the absence of this quality typifies what Lior Strahilevitz would call “charismatic code” design).<sup>143</sup> Instead, the user is invited to a “community” of peers who exchange song files. A user, importantly, has no sense that she is “selling” copyrighted materials. The design therefore exploits the distinction between the acceptance of non-commercial copying and the non-acceptance of commercial copying. While the economic consequences of peer filesharing could be large, the superficial absence of commercial exchange makes filesharing more acceptable under the norms of home copying.

### **Figure 3: The Friendly Face of the Bear-Share Community**

---

<sup>138</sup> See Office of Tech. Assessment, *supra* note 11, at 139–65.

<sup>139</sup> *Id.* at 163.

<sup>140</sup> *Id.*

<sup>141</sup> *Id.*

<sup>142</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 103, at 111–12.

<sup>143</sup> See Strahilevitz, *supra* note 12, at 549.



As an illustrative example, consider the BearShare client pictured above. There is little on the screen to suggest that a user is engaging in a morally ambiguous operation or is committing an act of theft. The friendly bear in BearShare is an icon of charismatic code.

The exploitation of social norms seems to have succeeded in facilitating a robust filesharing community. The 2000 Pew Internet Project Survey overwhelmingly supports the view that those who use filesharing networks do not think they are stealing.<sup>144</sup> That same study also suggests that fifty-three percent of all Internet users, and forty percent of all Americans, think that by sharing music through the Internet they are not doing anything wrong.<sup>145</sup> Along these same lines, a 2002 survey by Business Software Alliance found that only thirty-eight percent of Internet users claimed they would never download a potentially pirated program to save money.<sup>146</sup> In the end, P2P networks not only exploit the limits of legal enforcement, but also dodge the system of social norms that fortifies the relevant legal rules.

This Part has demonstrated that the success of P2P depends on the presence of certain vulnerabilities peculiar to copyright law. Part III considers the reaction of the beneficiaries of copyright law and the regulatory competition that followed it.

<sup>144</sup> Lenhart et al., *supra* note 11, at 5.

<sup>145</sup> *Id.* at 6.

<sup>146</sup> See Business Software Alliance, Survey Spotlights Growing Problem of Online Software Piracy, at [www.bsa.org/resources/2002-05-29.117.pdf](http://www.bsa.org/resources/2002-05-29.117.pdf) (May 29, 2002) (on file with the Virginia Law Review Association).

## III. THE EVOLUTION OF P2P DESIGN AND REGULATORY COMPETITION

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

There are two outstanding aspects to this story. The first is the degree to which code design evolved to better target the weaknesses of the copyright regime. Part II demonstrated that P2P networks were generally designed to target copyright's dependence on a gatekeeper system and to exploit the lack of clear normative support for the copyright system. This Part will show that the design evolved to take advantage of a specific legal doctrine—copyright's contributory liability doctrine—embodied in the decision in *Sony Corp. of America v. Universal City Studios*,<sup>147</sup> and elaborated in *A & M Records v. Napster*.<sup>148</sup>

The second is the nature of the reaction to the P2P network. The recording industry is obviously the beneficiary of the existing copyright laws, and the erosion of the gatekeeper regime provoked an investment in various mechanisms of legal change (investments in efforts to change copyright law). These patterns follow the model of regulatory competition described in Part I.

A. *Napster and its Predecessors*

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 available for download. The company “MP3.com,” which debuted in 1996, is one well-known example. Its “My.MP3” service allowed users to download, among other things, copyrighted MP3 files, provided they owned the CD that corresponded to the file in question.<sup>149</sup> This service effectively gave users remote access to music that they already owned.

---

<sup>147</sup> 464 U.S. 417 (1984).

<sup>148</sup> 114 F. Supp. 2d 896 (N.D. Cal. 2000).

<sup>149</sup> See Lawrence Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* 192 (2001).



The architecture of My.MP3 and other web-based services, not the fair-use issue, is of particular interest here.<sup>150</sup> My.MP3 relied on a pure client-server model. It placed a huge amount of copyrighted material in a single space. When the recording industry sued, the company's activities were deemed clearly illegal under the traditional model of copyright enforcement.<sup>151</sup> The recording industry's case was not much different, enforcement-wise, from the Elvis bootleggers in *Dowling v. United States*<sup>152</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>153</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>154</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>155</sup>

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 differentiated itself from the traditional commercial copyright pirate by styling itself as a place to trade music rather than as a place to sell or distribute it.

Napster, however, was not completely decentralized. Napster's programmers, Shawn Fanning and Jordan Ritter, were also aware of the

---

<sup>150</sup> Because 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 *id.* at 193–94.

<sup>151</sup> See *UMG Recordings v. MP3.com, Inc.*, 92 F. Supp. 2d 349, 350 (S.D.N.Y. 2000).

<sup>152</sup> 473 U.S. 207 (1985).

<sup>153</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 5D, available at 1998 WL 5740934 (noting the "abundance of sites both legal and illegal").

<sup>154</sup> For example, the website MP3Board offered a search engine for such sites and was quickly sued. See *MP3Board v. Recording Indus. Ass'n of Am.*, No. C-00-20606RMW, 2001 WL 804502, at \*3 (N.D. Cal. Feb. 27, 2001) (staying a California countersuit).

<sup>155</sup> Shirky, *supra* note 125, at 28.

challenge to P2P networks of operating on a mass scale.<sup>156</sup> Napster mixed client-server and peer elements in order to make the search for songs a fast and scalable solution. Hence, the Napster server facilitated both database searching and brokering of individual connections.

The design scaled impeccably. While estimates vary, at its height, Napster had tens of millions of active users, an astonishing technological accomplishment.<sup>157</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>158</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 have been different if Napster had been a form of multi-purpose copying technology over which Napster itself had no specific power. This relationship between technology and ownership 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>159</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 because the equipment has substantial non-infringing uses, they are not made liable.<sup>160</sup>

Napster’s argument—that it was a mere instrument of both legal and illegal uses—was belied by its design. One overriding factual finding doomed the company: The court found that “[Napster] could block access to the system by suppliers of the infringing material.”<sup>161</sup>

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

---

<sup>156</sup> See Jordan Ritter, Why Gnutella Can’t Scale. No, Really., at <http://www.darkridge.com/~jpr5/doc/gnutella.html> (Feb. 2001) (on file with the Virginia Law Review Association) (discussing scaling problems in P2P networks).

<sup>157</sup> See Healey, *supra* note 93.

<sup>158</sup> See *A & M Records v. Napster, Inc.*, 114 F. Supp. 2d 896, 900 (N.D. Cal. 2000).

<sup>159</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>160</sup> The *Sony* Court described this as the “staple article of commerce doctrine.” *Id.*

<sup>161</sup> *A & M Records v. Napster, Inc.*, 239 F.3d 1004, 1022 (9th Cir. 2001). See also *id.* at 1023 (“The district court correctly determined that Napster had the right and ability to police its system.”).

play despite having the power to stop the performance.<sup>162</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>163</sup>

After the court found that Napster exercised control, holding it 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>164</sup> The record industry sent Napster notice of thousands of infringing files available through the system and then proved that these files remained available for download.<sup>165</sup>

On the issue of vicarious liability, the decisive legal question also involved Napster’s degree 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>166</sup> Napster’s architecture again provided an answer. As the court noted, “Napster retains the right to control access to its system.”<sup>167</sup>

This ruling led Napster to bankruptcy<sup>168</sup> and also taught several legal lessons to P2P code designers. 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. Napster looked like a pretty good idea a year ago, but today Gnutella and Freenet look like much better ideas.”<sup>169</sup> *Napster* taught peer network designers that both lack of control and general functionality had to be

---

<sup>162</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>163</sup> *Sony*, 464 U.S. at 437.

<sup>164</sup> *Napster*, 239 F.3d at 1020. This formula has become the favored technique for proving knowledge in service provider cases. See *Religious Tech. Ctr. v. Netcom On-Line Communication Servs.*, 907 F. Supp. 1361, 1373–75 (N.D. Cal. 1995) (allowing actual knowledge to be demonstrated in this manner).

<sup>165</sup> *Napster*, 239 F.3d at 1022.

<sup>166</sup> *Id.* at 1022 n.6.

<sup>167</sup> *Id.* at 1023.

<sup>168</sup> The Ninth Circuit’s ruling on the preliminary injunction was the effective, but not the formal, end of the litigation over Napster. See *A & M Records v. Napster, Inc.*, 284 F.3d 1091, 1099 (9th Cir. 2002) (affirming the district court’s preliminary injunction).

<sup>169</sup> Kan, *supra* note 125, at 121.

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, *Napster* suggested, should take the form of a protocol rather than an application. Email and Usenet had never been sued for copyright infringement, despite their widespread use for illegal purposes. The lesson was simple—Napster had not gone far enough.

There was a flurry of attempts to succeed Napster; many so technologically unsuccessful (*Napigator*) or so clearly liable under *Napster* (*Scour*) as to be unworthy of discussion. Over the years 1999-2002 there were approximately fifty-eight different filesharing clients released to the market.<sup>170</sup> Of those, only four or five have enjoyed lasting significance.<sup>171</sup> One successor was different. It was founded on concepts of radical decentralization and was 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>172</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>173</sup> Gnutella delivered a radi-

---

<sup>170</sup> The compiled list of filesharing clients from 1999–2002 includes: Abe’s MP3 finder, Aimster (now named Madster), Ares, Audio-Galaxy, AudioGnome, BadBlue, Bearshare, Blubster, CuteMX.Com, DirectConnect, eDonkey, FileAngel, Filetopia, File Navigator, File Rogue, FileSpree, Free Haven, Freenet, Frost, Gnotella, Gnucleus, Gnutella 0.56, Gnutmeg, Grokster, Groove Network, Hotline Communications, iMesh, iSwipe, Junge Monkey, Ka-ZaA, KonSpire, Limewire, Mactella, Mojo Nation, Morpheus, MyNapster, Myster, NapMX, Napster, Nutella, Ohaha, OnSystem, OpenNap, Phex, Phosphor, Pointera, Publius, Qtella, 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>171</sup> In focusing on the major developments, some might argue that I have shortchanged programs like Scour.com and Aimster in the process.

<sup>172</sup> Kan, *supra* note 125.

<sup>173</sup> Gnutella was released in March of 2000. It was invented by Justin Frankel and Tom Pepper, two programmers working for AOL’s Nullsoft. *Id.* 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, at <http://www.oreillynet.com/lpt/a/208> (May 5, 2000) (on file with the Virginia Law Review

cally decentralized design that made it a darling of academic study. The design was an intentional effort to create a filesharing protocol that could avoid a lawsuit. Although it succeeded, it did so at the expense of social and scalability problems.

Gnutella's decentralization was nearly absolute. No single node on the early Gnutella network was different than any other. Searching, file transferring, and peer finding were all accomplished without the creation of specialized intermediaries. The only identifiable intermediaries were those relatively limited 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 whomever happens to be nearby.<sup>174</sup> The design implements the idea that "Gnutella is not a program, it is a *protocol*."<sup>175</sup> In other words, Gnutella's designers created a filesharing network—GnutellaNet—that was unowned and uncontrolled and to which various Gnutella programs could provide access. The relationship between the application and the network was similar to that between various email programs (Eudora, Microsoft Outlook, Hotmail) and the one-serves-all email network that cannot be said to be owned by anyone. GnutellaNet was designed as a general filesharing network capable of sharing any computer file.<sup>176</sup>

Gnutella was a success on the legal front. Gnutella's radical decentralization avoided the legal liability that had plagued Napster. To date, neither GnutellaNet nor its main application designers have been sued,<sup>177</sup> despite the substantial volume of infringement they facilitate.

---

Association). Gnutella's full development followed (and still follows) the non-linear path characteristic of open-source code. *Id.*

<sup>174</sup> See Kan, *supra* note 125, at 97–98.

<sup>175</sup> From Strategic Vision to a 10-Point Tactical Plan: A followup to The Revolution Will Be Webcast (working paper), at <http://economicdemocracy.org/counterspinner.html> (last visited Mar. 20, 2003) (on file with the Virginia Law Review Association).

<sup>176</sup> This characteristic was even more evident in another network, FreeNet, aimed at achieving the goals of the World Wide Web (storage of information) in a decentralized, purely P2P 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 46 (Hannes Federrath ed., 2001); see also Adam Langley, Freenet, *in* Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology, *supra* note 123, at 123 (describing the development and structure of Freenet).

<sup>177</sup> It is true that Morpheus switched to Gnutella after it was sued as one of the three Fast-Track companies, but no Gnutella developer qua Gnutella developer has been sued.

The early GnutellaNet, however, 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>178</sup> The 2000 crash was the first sign that the early Gnutella client design had traded resistance to litigation for system instability.

Commentators quickly diagnosed the problem.<sup>179</sup> Early GnutellaNet's stability relied on users' willingness to donate both bandwidth and music files to a common cause and to limit judiciously their own use of the network. Once a certain number of users joined the network, stark differences in user bandwidth and the lack of a central mechanism for allocating traffic to more capable users made a crash inevitable. While some touted the theoretical scaling capabilities of Gnutella,<sup>180</sup> the instability of early GnutellaNet was undeniable. In addition to the scaling problem, there were also "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 seventy percent of Gnutella users shared no files and that nearly fifty percent of all responses were returned by the top one percent of sharing hosts.<sup>181</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.

---

<sup>178</sup> See Steve McCannell, *The Second Coming of Gnutella*, WebReview (Mar. 2, 2000), at [http://www.webreview.com/mmedia/2001/03\\_02\\_01.shtml](http://www.webreview.com/mmedia/2001/03_02_01.shtml) (on file with the Virginia Law Review Association) (detailing reasons for the crash). Interestingly, the crash came directly in the wake of the *Napster* injunction as thousands 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.

<sup>179</sup> See *id.*; Matei Ripeanu, *Peer-to-Peer Architecture Case Study: Gnutella Network*, at [http://www.cs.uchicago.edu/files/tr\\_authentic/TR-2001-26.pdf](http://www.cs.uchicago.edu/files/tr_authentic/TR-2001-26.pdf) (last visited Mar. 20, 2003) (on file with the Virginia Law Review Association) (describing Gnutella's scaling problems); Ritter, *supra* note 156; See also Hong, *supra* note 123, at 206–07 (summarizing a now unavailable Clip2 study of the crash). A network engineer would diagnose 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 available resources.

<sup>180</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, *supra* note 125, at 109–17.

<sup>181</sup> Eytan Adar & Bernardo A. Huberman, *Free Riding on Gnutella*, 5 *First Monday* 10 (Oct. 2000), at [http://www.firstmonday.dk/issues/issue5\\_10/adar/index.html](http://www.firstmonday.dk/issues/issue5_10/adar/index.html) (on file with the Virginia Law Review Association).

The problems of Gnutella 2000 were generally recognized,<sup>182</sup> yet Gnutella's failures were not the end of the peer filesharing response. The crashes and instability led to a new generation of peer filesharing software. These new-generation programs, bearing names such as KaZaA, Grokster, Morpheus, and BearShare, are, for now, the latest chapter of the peer response story.

### *C. The KaZaA Era: 2001 - Present*

The legal vulnerabilities of Napster and the stability and social problems of Gnutella inspired a new approach. Led by the enigmatic KaZaA, and its FastTrack engine, 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 doomed Napster. The results are programs of great sophistication, attuned carefully to the doctrines of copyright.

The new generation reintroduced hierarchy among users. They created a distinction between "regular peers" and "superpeers" based on detected resources—in particular, bandwidth.<sup>183</sup> In this hierarchy, college students are on top: high bandwidth users (college students on university networks, home DSL, and cable users) are superpeers, while dial-up users (home modem users) are regular peers.

Dozens of programs grew into the technological gap between Napster and Gnutella. Only a few, however, reached mass scale for any length of time.<sup>184</sup>

#### *1. FastTrack & KaZaA*

FastTrack returned filesharing to an enterprise of substantial scale. In late 2001, the FastTrack network grew to be the largest filesharing network since Napster, with an average of two to four million users online

---

<sup>182</sup> See Hong, *supra* note 123, at 206–07; McCannell, *supra* note 178; Ripeanu, *supra* note 179.

<sup>183</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 Feb. 9, 2003) (on file with the Virginia Law Review Association).

<sup>184</sup> Some of the more major programs from this period not discussed here include Audio-Galaxy, Aimster (now named Madster), WinMX, iMesh, and OpenNAP.

at any given time.<sup>185</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>186</sup> Unlike Gnutella, the protocol was never released as an open-source standard.<sup>187</sup> Instead, KaZaA insisted that companies pay to access the FastTrack network. The companies Grokster and Morpheus<sup>188</sup> did so, creating several client alternatives.

The FastTrack companies fit somewhere between early Gnutella and Napster in their elimination of intermediaries. The protocol borrows heavily from Gnutella. It also maintains the distinction between the protocol and the clients; the company KaZaA, for instance, maintains no power to “shut down” the network.<sup>189</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, from user accounts, produces much better performance than even the next-generation Gnutella clients.<sup>190</sup> Such tiering, however, 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 in to the system (in order to maintain statistics), and helping the process of finding peers in the first place. As previously discussed, efficient operation is difficult to maintain in the face

---

<sup>185</sup> This number is based on Active Users statistics, at [www.sylk.com](http://www.sylk.com) (July 22–Aug. 8, 2002) (on file with the Virginia Law Review Association).

<sup>186</sup> Kevin Maney, *Fight over digital music filesharing keeps getting weirder*, USA Today, Sept. 25, 2002, at B3.

<sup>187</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) (on file with the Virginia Law Review Association) (describing giFT and OpenFT).

<sup>188</sup> See Benny Evangelista, *Morpheus software morphing: Maker of filesharing program put limits on MP3 swapping*, S.F. Chron., Mar. 14, 2002, at B1. Morpheus later reverted to Gnutella, after licensing disagreements with KaZaA. See *id.*

<sup>189</sup> See Amy Harmon, *Music Industry in Global Fight on Web Copies*, N.Y. Times, Oct. 7, 2002, at A1.

<sup>190</sup> See, e.g., *Morpheus 2.0—Revisited*, Slyck, at <http://www.slyck.com/newsaug2002/081902b.html> (Aug. 19, 2002) (on file with the Virginia Law Review Association) (discussing loss of performance when Morpheus switched from FastTrack to Gnutella network).



of radical decentralization.<sup>191</sup> Third, at least one of the FastTrack companies (KaZaA) promotes 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>192</sup> The study demonstrated that many users were sharing all of the files on their computers, but were totally unaware of that fact.<sup>193</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>194</sup> KaZaA's parent is incorporated in Vanuatu, a group of islands in the South Pacific noted for its lack of a copyright law. Grokster maintains its servers in Nevis, a thirty-six square mile nation-state in the West Indies. Only Morpheus resides in the United States.<sup>195</sup>

## 2. Next-Generation Gnutella

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. Gnutella responded to its scaling and social problems by adopting a superpeer design similar to that of FastTrack. The best known of the new GnutellaNet developers are Bearshare and Limewire. Both compromise a purely decentralized design of equal users by distinguishing between high- and low-bandwidth users and by giving the former more duties.

The continued growth of Gnutella was marked by a lack of coordination among developers. As Kelly Truelove writes, “Unfortunately, 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>196</sup>

---

<sup>191</sup> See *supra* text accompanying notes 172–82.

<sup>192</sup> Nathaniel S. Good & Aaron Krekelberg, Usability and privacy: a study of Kazaa P2P file-sharing, HP Laboratories, at <http://www.hpl.hp.com/techreports/2002/HPL-2002-163.pdf> (June 5, 2002) (on file with the Virginia Law Review Association).

<sup>193</sup> *Id.*

<sup>194</sup> See Harmon, *supra* note 189, at A1.

<sup>195</sup> See *id.*

<sup>196</sup> Kelly Truelove, Gnutella: Alive, Well, and Changing Fast, OpenP2P.com, at <http://www.openp2p.com/pub/a/p2p/2001/01/25/truelove0101.html?page=2> (Jan. 25, 2001) (on file with the Virginia Law Review Association).

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 GnutellaNet.<sup>197</sup> These efforts, as was the case with the FastTrack companies, may make these clients easier to sue because they suggest an increased quantum of “control” over the Gnutella network.

Finally, despite the change, Gnutella still appears to have scaling problems. Statistics kept by Limewire show that, during the first half of 2002, the network size rarely reached more than 500,000.<sup>198</sup> By July 2002, GnutellaNet had declined to an average of 160,000 nodes.<sup>199</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>200</sup> These concerns show the continuing difficulty in balancing decentralization and selfless behavior. Yet the fact that GnutellaNet remains unsued endows it with an aura of continued importance in the filesharing story.

#### D. FastTrack and Gnutella Go to Court

On October 2, 2001, the music industry sued Grokster, Morpheus, and KaZaA: the three principal FastTrack companies.<sup>201</sup> This ongoing lawsuit is a signal test of the viability of designing code to avoid legal liability. Programmers wrote FastTrack and Gnutella to exploit loopholes left by the *Napster* decision. The case, styled *Metro-Goldwyn-Mayer Studios v. Grokster*, asks whether the P2P programmers have succeeded. The initial answer is yes.

The music industry’s complaint made every effort to stress the similarity between Napster and KaZaA and the other FastTrack companies.

---

<sup>197</sup> Namely, the clients Gnutella and Gnutella.it allowed users simply to use GnutellaNet to download files. See *id.*

<sup>198</sup> Gnutella’s Decline, Slyck, at <http://www.slyck.com/newsjuly2002/071702a.html> (July 17, 2002) (on file with the Virginia Law Review Association).

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

<sup>200</sup> *Id.*

<sup>201</sup> Complaint for Damages and Injunctive Relief for Copyright Infringement at 2, 8, *Metro-Goldwyn-Mayer Studios v. Grokster*, 2003 WL 186657 (C.D. Cal. Jan. 9, 2003) (No. Civ.01-08541) (seeking damages and injunctive relief for copyright infringement), available at [http://www.mpaa.org/Press/KaZaA\\_Complaint.htm](http://www.mpaa.org/Press/KaZaA_Complaint.htm) (last visited Feb. 9, 2003) (on file with the Virginia Law Review Association).

Once again it accused the companies of creating “a 21st century piratical bazaar.” It noted that the defendants grant access to “a closed computer network, controlled by Defendants.”<sup>202</sup> It also put emphasis of the fact that communications are centrally encrypted.<sup>203</sup> The complaint highlights these facts to support the argument that the FastTrack companies, like Napster, “are capable of controlling the activities of their users.”<sup>204</sup>

But the facts did not support this contention (by design). District Judge Stephen Wilson, granting summary judgment in favor of Grokster and Morpheus,<sup>205</sup> refused to buy the comparison to Napster (the program). The opinion suggests that the changes in design “worked,” at least with respect to negating the element of control that sealed Napster’s fate.

Just as in *Napster*, the court took the issue of control as the sine qua non of contributory liability. As the court put it: “[T]he critical question is whether [defendants] do anything, aside from distributing software, to actively facilitate—or whether they could do anything to stop—their users’ infringing activity.”<sup>206</sup> It was here that the changes in design made a difference. Judge Wilson pointed out, in a crucial factual holding:

Neither StreamCast nor Grokster facilitates the exchange of files between users in the way Napster did. Users connect to the respective networks, select which files to share, send and receive searches, and download files, all with no material involvement of Defendants. If either Defendant closed their doors and deactivated all computers within their control, users of their products could continue sharing files with little or no interruption.<sup>207</sup>

As noted above, Gnutella and FastTrack embody a self-conscious effort to make P2P filesharing more like the VCR or photocopier. And the court accepted just that rationale, concluding, “Grokster and StreamCast are not significantly different from companies that sell home video recorders or copy machines, both of which can be and are used to

---

<sup>202</sup> Id. (seeking damages and injunctive relief for copyright infringement).

<sup>203</sup> Id. at 2–3.

<sup>204</sup> Id. at 10.

<sup>205</sup> See *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, \_\_F. Supp. 2d\_\_, 2003 WL 1989129 (C.D. Cal. Apr. 25, 2003). Default judgment was entered against a shell company named KaZaA BV, holding no relevant assets, who declined to defend the lawsuit. See id. at 4 n.2. Sharman Networks, the current operator of the KaZaA system, was not a party to the motions. See id. at 6.

<sup>206</sup> Id. at 19.

<sup>207</sup> Id. at 23–24.

orders or copy machines, both of which can be and are used to infringe copyrights.”<sup>208</sup> Hence, “absent evidence of active and substantial contribution to the infringement itself, Defendants cannot be liable.”<sup>209</sup>

Will the judgment survive appeal? There are reasons to suspect it will not. The district court’s decision ultimately depends on *Sony* as interpreted by *Napster*. *Sony* in turn, can be read as a policy judgment aimed principally at correcting a perceived market failure.<sup>210</sup> While clearer in hindsight, it is apparent that the *Sony* decision correctly addressed a market failure.<sup>211</sup> The VCR broadened the addressable market for television shows (via time-shifting) and for movies (via rentals). Though there is an argument that filesharing helps the music industry, the desirability of the “help” is much less apparent.<sup>212</sup> Filesharing looks more like a replacement for legitimate music sales; such reasoning may compel a court to find some way to assess liability on P2P developers regardless of the *Napster* precedent. In addition, the ratio of infringing to non-infringing use must be at the forefront of the ultimate policy judgment in this area. If the alleged non-infringing uses retain their de minimis character the Court of Appeals will presumably feel that there is little consequence in ruling against the P2P filesharing companies.

Perhaps the only policy reason to think otherwise is an institutional argument. Ultimate settlement of the filesharing dispute, the argument goes, is a task for Congress; and a decision against the copyright owners will force such settlement. Such “settlement-forcing” decisions in copyright have a long pedigree, from the 1908 piano-roll case *White-Smith Music Publishing Co. v. Apollo Co.*,<sup>213</sup> to the cable-broadcast decisions of the 1960s and 1970s.<sup>214</sup> Both prompted Congressional action to settle a dispute between an incumbent and challenger technology.<sup>215</sup> Judge

---

<sup>208</sup> *Id.* at 27.

<sup>209</sup> *Id.*

<sup>210</sup> See 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).

<sup>211</sup> See *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, 260–63 (2001) (giving the basic economic argument that *Napster* be held liable and suggesting Coasean complications).

<sup>212</sup> For studies supporting this position, see Chipman, *supra* note 98; Lahey, *supra* note 98.

<sup>213</sup> 209 U.S. 1 (1908).

<sup>214</sup> See *Fortnightly Corp. v. United Artists*, 392 U.S. 390 (1968); *Teleprompter Corp. v. Columbia Broad. Sys., Inc.*, 415 U.S. 394 (1974).

<sup>215</sup> See 17 U.S.C. §§ 111, 115 (cable and mechanical compulsory licenses).

Wilson clearly had this in mind, writing “[w]hile the Court need not decide whether steps could be taken to reduce the susceptibility of such software to unlawful use . . . additional legislative guidance may be well-counseled.”<sup>216</sup> It remains to be seen whether the Courts of Appeals will think that trying to force settlement of copyright disputes remains an appropriate court function.

### *E. The Reaction to the Reaction*

The recording industry’s reactions to P2P filesharing is a paradigm for understanding the modern face of regulatory competition. As preceding Sections have shown, the filesharer’s comparative advantage lay in designing code to avoid copyright law. The recording industry, meanwhile, has invested in a broader range of mechanisms to influence law and its effects. The content industry invested in changing the law (by controlling access, increasing intermediary liability, and increasing criminal liability), in changing social norms, and in changing code to attack P2P networks. The extent of increased investment can be seen from the annual increases in the budget of the RIAA itself. In the early 1990s, the RIAA’s budget was estimated at \$10 million.<sup>217</sup> By 1995, the RIAA was spending \$14.7 million. By 2000, the budget had tripled to \$39 million and in 2001 stood at \$44 million.<sup>218</sup>

#### *1. Investments in Change*

The recording industry’s investments in legal change are most prominent. In the 1990s, the content industry invested considerable time and energy to ensure the passage of three critical laws to buttress copyright enforcement: the anti-circumvention provisions of the DMCA,<sup>219</sup> the ISP-liability sections of that same bill,<sup>220</sup> and the enhancement of copyright’s criminal penalties in the No Electronic Theft (“NET”) Act.<sup>221</sup>

The anti-circumventions provisions of the DMCA reinforce various technological techniques of preventing copying by criminalizing cir-

---

<sup>216</sup> *Grokster*, \_\_F. Supp. 2d\_\_ at 33.

<sup>217</sup> See Bill Holland, Tougher RIAA gives pirates chase but still running uphill, *BillBoard*, Mar. 14, 1992, available at 1992 WL 11645300.

<sup>218</sup> See Bill Holland, Performers Give Testimony Before Judges And Lawmakers, *BillBoard*, Sept. 22, 2001, available at 2001 WL 24692410.

<sup>219</sup> 17 U.S.C. § 512(1998).

<sup>220</sup> 17 U.S.C. § 512(1998)

<sup>221</sup> 17 U.S.C. §§ 101, 506 (2000).

cumvention of copy protection systems.<sup>222</sup> The provisions can be understood as an effort to restore an eroding gatekeeper system. Technological copy protection “respecializes” the creation and mass distribution of copyrighted works, while the DMCA’s anti-circumvention law makes it a crime to undo the respecialization.<sup>223</sup> The law can be understood as an effort to return content owners to the 1970s, when they were free to sit back and police the few intermediaries licensed to access the copy-protected content.<sup>224</sup> The anti-circumvention provisions are usually discussed in conjunction with the much-discussed possibility of effective digital rights management.<sup>225</sup> Some have speculated that there may be a future where content owners manage to encrypt content so carefully and comprehensively from the outset, and maintain their control continuously, that the code prevents infringement *ex ante*.<sup>226</sup> Such efforts remain in their early stages and are highly speculative, but they would eventually transform the economics of copyright enforcement.<sup>227</sup>

The ISP-specific sections of the DMCA, Section 512 *et seq.*, represent the culmination of an effort to replace the lost intermediaries of times past with ISPs. There have been a few attempts to use these sections to target filesharing. In the summer of 2002, the RIAA filed a lawsuit against various telephone companies who operate the backbone of the Internet, based on their failure to contain overseas copyright infringement, but it dropped the suit a week later.<sup>228</sup> More recently, using a

---

<sup>222</sup> See 17 U.S.C. § 1201 (1998).

<sup>223</sup> A more recent example in the same vein is the well-known “Hollings Bill.” Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. (2002). The bill would require all “digital media devices” to include copy protection technology in their designs. *Id.* § 5(a). It can be otherwise described as an effort to place the burden of preventing copyright infringement on electronics manufacturers.

<sup>224</sup> It is worth briefly noting, however, that there is a problem with the DMCA strategy as a response to filesharing. Unless completely successful in blocking access, digital protection schemes can simply make legal, protected products even less attractive than the competitors available through filesharing networks.

<sup>225</sup> See, e.g., Lessig, *supra* note 149, at 177–99; see also Raymond Ku, *The Creative Destruction Of Copyright: Napster And The New Economics Of Digital Technology*, 69 *U. Chi. L. Rev.* 263, 275–76 (2002) (describing digital rights management systems).

<sup>226</sup> These ideas are explored more fully in Lessig, *supra* note 149, at 177–99.

<sup>227</sup> Cf. Ku, *supra* note 225, at 275–76 (arguing against copyright protection for digital works because the economics of digital technology undercuts prior assumptions about the efficacy of a private property regime for information).

<sup>228</sup> Alex Pham, *Tactics Toughen on Music Piracy*, *L.A. Times*, Aug. 21, 2002, at C1; Alex Pham, *Technology RIAA Drops Suit Targeting Piracy Site*, *L.A. Times*, Aug. 22, 2002, at C5.

different section of the DMCA, 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>229</sup>

Finally, the efforts to pass the NET Act of 1997 and subsequent lobbying represent an effort to turn to the criminal side of copyright to enhance primary enforcement. Under the little-noticed NET Act, the federal government may criminally prosecute relatively minor copyright infringements.<sup>230</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>231</sup> This definition makes quid pro quo filetrading potentially criminal.

Copyright owners have mounted an effort to convince the Justice Department to enforce the NET Act against individual peer filesharers.<sup>232</sup> This amounts to an attempt to increase the sanction, if not the probability of detection, for copyright infringement. The untested question remains whether either criminal or civil primary enforcement will be effective in deterring illegal P2P filesharing, given the limits of primary enforcement in producing deterrence.<sup>233</sup>

## 2. *Extralegal Investments*

In addition to legal changes, the recording industry has also invested in trying to change the social norms surrounding copyright infringement and has made some efforts to combat P2P filesharing directly. As discussed above,<sup>234</sup> when it comes to copying files, people have proven to be unaffected by the ethical tug of the copyright statute. The software and recording industries have spent a decade trying to change that atti-

---

<sup>229</sup> *In re Verizon Internet Services*, No. Civ.A.02-MS-0323, 2003 WL 141147 (D.D.C. Jan. 21, 2003).

<sup>230</sup> 17 U.S.C. §§ 101, 506 (2000).

<sup>231</sup> *Id.* § 101.

<sup>232</sup> See Benny Evangelista, *Casting a wider net/Recording industry may target individuals in online piracy battles*, S.F. Chron., Aug. 22, 2002, at E1, available at 2002 WL 4028698 (recounting efforts to have the Justice Department enforce the criminal side of copyright law).

<sup>233</sup> See Lisa M. Bowman, *File-traders in the crosshairs*, CNET News, at <http://news.com/2100-1023-943881.html> (July 15, 2002) (on file with the Virginia Law Review Association) (reporting that the recording industry is considering a program of lawsuits against end-users).

<sup>234</sup> See discussion *supra* Section II.E.

tude. The RIAA's "Sound-Byting" campaign, for example, is an investment to try to change the attitudes of college students toward copyright infringement. The central message of this campaign is: "[U]ploading and downloading somebody else's music without their permission isn't just against the law. It's a rip-off. Simple as that."<sup>235</sup> Hilary Rosen, the President of the RIAA, even participated in a well-publicized public debate at Oxford, arguing that illegal filesharing is immoral.<sup>236</sup> As the statistics cited here and the Pew Internet Project Study discussed above indicate,<sup>237</sup> it is unclear whether these efforts have had much success in changing public attitudes toward filesharing.

Perhaps most interestingly, content owners may also be taking a page from the book of P2P designers themselves, using code to influence the enforcement of copyright law by attacking the P2P networks that undermine copyright enforcement. Reports on the use of attacks on P2P networks are hard to verify. However, there are several methods through which content owners might try to disable P2P networks. One method seeks to decrease the attractiveness of P2P networks, often by flooding the network with dummy or broken music files.<sup>238</sup> Users then must spend more time looking for good files, increasing the attractiveness of conventional distribution channels. Another method would simply attack important network nodes using techniques familiar to computer hackers.<sup>239</sup> More fanciful examples of this type of strategy include that of a virus designed to detect illegally copied materials.<sup>240</sup> The extent to which these methods are used today is a carefully guarded secret.<sup>241</sup> The continued activity of peer filesharing networks, however, suggests either limited success or limited usage of such techniques.

---

<sup>235</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>236</sup> See Matt Bai, Hating Hilary, *Wired* 11.02 (Feb. 2003), at [http://www.wired.com/wired/archive/11.02/hating\\_pr.html](http://www.wired.com/wired/archive/11.02/hating_pr.html) (on file with the Virginia Law Review Association).

<sup>237</sup> See *supra* text accompanying note 130.

<sup>238</sup> For an entertaining account of how anonymity can be used against peer networks, see Doug Lichtman & David Jacobson, Anonymity a double-edged sword for pirates on-line, *Chi. Trib.*, Apr. 13, 2000, at 25.

<sup>239</sup> For example, a "Denial of Service" attack, which floods a given network node with requests.

<sup>240</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>241</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> (on file with the Virginia Law Review Association) (surveying methods of technological self-help).



On June 25, 2002, Representative Howard Berman of North Hollywood, California proposed that “[t]echnological self-help” should help provide the solution to “unbridled” peer network piracy.<sup>242</sup> He proposed a bill that would give legal license for copyright owners to disrupt peer networks.<sup>243</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>244</sup>

The Berman bill, while unlikely to pass, shows the dramatic extent and even creativity of efforts to gain advantage in the regulatory competition surrounding copyright.

The story of the competition between the RIAA and P2P users delivers a snapshot of the future of understanding compliance and legal effects. A law’s meaning and effects, success or failure, seem ever less a function of drafting or enforcement. Rather, the question is what forces—social, economic, technological or otherwise—may be recruited for or against the cause.

#### IV. THE SOCIAL DYNAMICS OF P2P FILESHARING

“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>245</sup>

Over the last four years, P2P networks have provided a sub-group of media consumers with the equivalent of a temporary repeal of copyright laws for the technologically inclined. How can one explain the growth

---

<sup>242</sup> Press Release, Representative Howard Berman, Berman Announces Legislation To Foil Peer To Peer Piracy, at <http://www.house.gov/berman/pr062502.htm> (June 25, 2002) (on file with the Virginia Law Review Association).

<sup>243</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>244</sup> Press Release, *supra* note 242.

<sup>245</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) (Oct. 3, 2001) (on file with the Virginia Law Review Association).

and popularity of the peer filesharing movement? This final Part analyzes the particular fit between P2P filesharing and its beneficiaries. It shows first, that P2P may represent the rational exploitation of the larger group of music consumers by a subset of computer savvy P2P users, and second, that peer filesharing uniquely suited the disorganized nature of copyright consumers as a group.

#### A. Copyright's Divided Subjects

One reason P2P filesharing may have been successful is because users rationally exploited “regular” consumers who lack the knowledge or resources to use P2P networks. In the standard (if sometimes disputed) account, copyright law is said to serve the interests of content consumers.<sup>246</sup> The law provides financial and, debatably, expressive incentives to create materials that would otherwise not exist. If this is right, why would consumers ever want to disobey copyright law?

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 *collective* interest of consumers, it is not in any given individual's 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>247</sup> to refer to the fact—confirmed by empirical

---

<sup>246</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. For examples of such positions see, e.g., Eben Moglen, *Liberation Musicology*, *The Nation*, Mar. 12, 2001, at 5; Mark S. Nadel, *Questioning The Economic Justification For (and Thus Constitutionality of) Copyright Law's Prohibition Against Unauthorized Copying: § 106* (unpublished manuscript), at <http://www.aei.brookings.org/admin/pdf/Nadel.pdf> (Jan. 2003) (on file with the Virginia Law Review Association); 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).

<sup>247</sup> The question of who coined the term “digital divide” remains something of a mystery. See Sharon Foster & Adrianna Borkowski, *Who Coined the Term?*

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 more likely to own a computer than those without any high school education (63.2% vs. 6.8%).<sup>248</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>249</sup>

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

It is unlikely that the programmers of Napster and other applications actively considered the dynamics of collective action before writing code. But because filesharing remains confined to a limited group, filesharers can see that their actions will not eliminate all incentives to create music or seriously impoverish artists. Users of peer networks are a select group that could and still do live by slightly different rules.

### *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 Copyright Act is a leading example. The Act was the workproduct of a twenty-one-year-long negotiation between affected industry

---

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) (on file with the Virginia Law Review Association).

<sup>248</sup> See Nat'l Telecommunications and Info. Admin., *Falling Through The Net II: New Data On The Digital Divide 4* (July 1998).

<sup>249</sup> *Id.*

groups.<sup>250</sup> Studies suggest, however, that groups representing consumer interests had little or no influence on the shape of the 1976 Act. Professor Jessica Litman concluded, “[T]he citizenry’s interest in copyright and copyrighted works was too varied and complex to be amenable to interest-group championship.”<sup>251</sup>

These studies show what is obvious: For an average consumer, lobbying for copyright change is expensive, likely futile, and, even if successful, an impossible change on which to capitalize. 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, other than sometimes adhering to a common protocol, even necessarily need to work together or coordinate their efforts.<sup>252</sup>

It might be difficult to convince users to *contribute*, as opposed to *take*, from the common pool of shared songs. The process of sharing, however, has a relatively low cost. Moreover, as Professor Strahilevitz demonstrates, the design of P2P clients can lead users to believe that they are participating in a community, triggering norms of reciprocity.<sup>253</sup>

One salient question is whether the objective of collective action moves to writing the peer application itself (the Napster program, etc.). This shift does not seem to occur. First, provided that the program can be sold, the programmer can appropriate some of the value produced by the evasion of copyright law and can avoid the collective action problem. Second, even if the collective action problem persists, the investment needed to write a peer networking program may be small enough

---

<sup>250</sup> See Litman, *supra* note 103, at 48–63 (discussing the negotiations behind the 1976 Act); see also Jessica Litman, Copyright Legislation and Technological Change, 68 *Or. L. Rev.* 275, 279–82 (1989) (same).

<sup>251</sup> Litman, *supra* note 103, at 52.

<sup>252</sup> The creation of the protocols does represent a collective action problem if they are open (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 proven its ability to create public goods. See 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).

<sup>253</sup> See Strahilevitz, *supra* note 12, at 547–71.

---

that the programmer is motivated to write it if for no other reason than 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 incentive 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* remarked, he “reached a level of fame unprecedented for a 19-year old who is neither a sports hero nor a pop star.”<sup>254</sup> But the financial incentives for writing response programs have not proved overwhelming.<sup>255</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>256</sup>

More seasoned companies, however, question the advertising model. KaZaA, for example, depends on selling pop-up ads<sup>257</sup> and plans to harness and sell the unused computing resources of its millions of peered users (derisively referred to as a “spyware” strategy).<sup>258</sup> It has freely admitted that the online advertising model does not deliver enough revenue for it to support continued development.<sup>259</sup>

---

<sup>254</sup> Karl Taro Greenfeld, Meet the Napster, *Time*, Oct. 2, 2000, at 60.

<sup>255</sup> See John Borland, Rocky financial road awaits file swappers, CNET News.com, at <http://news.com.com/2102-1023-273245.html> (Sept. 21, 2001) (on file with the Virginia Law Review Association) (describing the failure of file swapping programs to make any money).

<sup>256</sup> WinMX Interview with Kevin Hearn, President, Front Code Technologies, Slyck, at <http://www.slyck.com/newsjuly2002/071002c.html> (July 10, 2002) (on file with the Virginia Law Review Association).

<sup>257</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> (on file with the Virginia Law Review) (describing KaZaA’s business model).

<sup>258</sup> This strategy is referred to as “spyware” because it pretends to be performing one function while actually performing another. Spyware also sometimes refers to programs that collect and store information about the user.

<sup>259</sup> *Id.*

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>260</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 processes in their effort to evade copyright laws. They may then, in a further twist, find their tools of copyright evasion turned against them.

Alternatively, programming a peer response may be inexpensive enough that some individuals will always be willing to undertake the project for their own personal benefit. 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 filesharing 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>261</sup>

As suggested by the change/avoidance dichotomy in Part I, one of the reasons for the success of P2P 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 the copyright system for all computer-savvy users. This fact explains the mass popularity of P2P among disorganized consumers. As a result, Napster and other programs have become an alternative to political lobbying less by choice than by default.

---

<sup>260</sup> For example, BearShare, at [www.bearshare.com](http://www.bearshare.com), already sells a "professional" version.

<sup>261</sup> Opinions on what motivates open-source programmers vary. See, e.g., Kollock, *supra* note 252, at 220–39 (describing a gift model); Eben Moglen, *Anarchism Triumphant: Free Software and the Death of Copyright*, 4 *First Monday* 8, at [http://www.firstmonday.dk/issues/issue4\\_8/moglen/index.html](http://www.firstmonday.dk/issues/issue4_8/moglen/index.html) (Aug. 2, 1999) (on file with the Virginia Law Review Association) (arguing that economics cannot explain why people write free software).

## CONCLUSION

Finding bold predictions for what political programming projects means for the future of governance is not difficult to do. 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>262</sup>

My own prophecies are somewhat more modest. The ways groups influence their government and the effects of its laws are changing. But the effects are ambiguous. 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. At worst, already-privileged computer users will simply find new ways to free-ride.

---

<sup>262</sup> See John Perry Barlow, *The Next Economy of Ideas*, *Wired* 8.10 (Oct. 2000).