

University of Pennsylvania Carey Law School

## Penn Law: Legal Scholarship Repository

---

Faculty Scholarship at Penn Law

---


8-25-2004

### On Software Regulation

Polk Wagner

*University of Pennsylvania Carey Law School*

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

 Part of the [Computer Law Commons](#), [Intellectual Property Law Commons](#), [Property Law and Real Estate Commons](#), [Science and Technology Law Commons](#), and the [Software Engineering Commons](#)

---

#### Repository Citation

Wagner, Polk, "On Software Regulation" (2004). *Faculty Scholarship at Penn Law*. 50.  
[https://scholarship.law.upenn.edu/faculty\\_scholarship/50](https://scholarship.law.upenn.edu/faculty_scholarship/50)

This Article is brought to you for free and open access by Penn Law: Legal Scholarship Repository. It has been accepted for inclusion in Faculty Scholarship at Penn Law by an authorized administrator of Penn Law: Legal Scholarship Repository. For more information, please contact [PennlawIR@law.upenn.edu](mailto:PennlawIR@law.upenn.edu).

# ON SOFTWARE REGULATION

R. POLK WAGNER<sup>†</sup>

*Forthcoming 78 S. CAL L. REV. \_\_ (2005)*

*Draft of August 25, 2004.*

*See <http://papers.pennlaw.net/> for updates.*

## ABSTRACT

*This Article develops a novel analytic framework for the evaluation of regulatory policy in cyberspace, flowing from a reconceptualization of cyberlaw's central premise: software code as complementary to law rather than its substitute. This approach emphasizes the linkage between law and software; for every quantum of legal-regulatory impact, there is a corresponding equilibria of regulation-by-software. The absence of a legal right will stimulate a technological response—and such incentives will moderate with increased rights. Rather than “code is law,” this is “code meets law.”*

*The implications of this methodological shift are explored in the context of the emerging (and intensely controversial) cyberproperty right—defined as the right to exclude others from one's network resources. The debate over whether (and how, and why) concepts of property rights can be extended to bits stored on web servers, email systems and the like is both deeply intertwined with technology and fundamentally comparative in nature, bringing the importance of understanding the regulatory costs and benefits of software (as compared to law) into sharp relief.*

*The analysis that emerges suggests that, contrary to much of the relevant scholarly literature (and perhaps counterintuitively), the availability of technological mechanisms to replace legal rights likely strengthens, rather than weakens, the case for legal regulation in the form of property rights. At least in this context, a software-centric regulatory approach is dominated by regimes premised on property-backed contractual relationships.*

*Considering the regulatory environment of cyberspace from this perspective may have profound effects on the way we think about the form and function of law online. The nature of cyberspace as particularly sensitive to emerging concerns about the tyranny of software suggests that the online environment might be more suited for a broad property rights regime than has been recognized to date.*

---

<sup>†</sup> Assistant Professor, University of Pennsylvania Law School. I am indebted to Dan Hunter, Jason Johnston, Mark Lemley, Larry Lessig, Kristin Madison, David Post, Peggy Radin, Reed Shuldiner, and participants at seminars at Stanford Law School, the University Pennsylvania Law School, and the Penn-Temple-Wharton Colloquium for helpful comments on earlier incarnations of this project. Kevin Goldman, Patrick Mirville, Ron Day and Bill Mulherin provided research assistance. All errors are my own. Comments appreciated: [polk@law.upenn.edu](mailto:polk@law.upenn.edu).

# ON SOFTWARE REGULATION

## TABLE OF CONTENTS

I	INTRODUCTION .....	1
II	THE LAW–SOFTWARE INTERFACE: AN ANALYTIC FRAMEWORK .....	7
	<i>A. Code Meets Law</i> .....	8
	<i>B. Equilibrium at the Law-Software Interface</i> .....	10
	<i>C. Implications of Code Meets Law I: Dynamic Effects</i> .....	13
	<i>D. Implications of Code Meets Law II: Unpredictability &amp; Uncertainty</i> .....	16
III	THE CASE AGAINST SOFTWARE: THE PUBLIC EFFECTS OF SOFTWARE REGULATION .....	21
	<i>A. Software and Regulatory Safety Valves</i> .....	23
	<i>B. Software and the Recognition of Enforcement Costs</i> .....	24
	<i>C. Scaling Software</i> .....	24
IV	SOFTWARE AND THE CHOICE OF LEGAL RULES .....	26
	<i>A. Property Rules, Liability Rules, and Legal Preemption</i> .....	27
	<i>B. Choosing the Form I: Normative Analysis</i> .....	31
	<i>C. Choosing the Form II: Instrumental Analysis</i> .....	36
	<i>D. Choosing the Legal Rule in Cyberspace</i> .....	38
V	THE CASE OF CYBERPROPERTY .....	40
	<i>A. The Legal-Software Landscape of Cyberproperty</i> .....	42
	<i>B. The Limited Impact of a Cyberproperty Rule, and the Importance of         Defaults</i> .....	45
	<i>C. The Flexibility Imperative</i> .....	49
	<i>D. The Public Good of Network Access</i> .....	49
	<i>E. Clarity, Stability and Certainty</i> .....	51
	<i>F. Choosing Among Forms of Legal Regulation</i> .....	51
	CONCLUSION .....	59
	<i>APPENDIX A: THE TECHNOLOGY OF SOFTWARE-ASSISTED CYBERPROPERTY</i>	

# ON SOFTWARE REGULATION

R. POLK WAGNER

## I

Above all else, the story of the field of cyberlaw is a tale of two *codes*: law and software. The most significant principle to emerge from the academic study of law on the Internet is the idea that software code—the applications, operating systems, and protocols that determine the way we experience the online world—is broadly substitutable for legal code—the regulatory infrastructure of society.<sup>1</sup> Code is law; architecture is control; software is power.

While there is no question that the basic point is correct, it is nonetheless the case that widespread acceptance of the “code is law” meme has perhaps obscured the kaleidoscopic relationship between legal code and software code.<sup>2</sup> For though it is certainly true that both software and law have important regulatory effects, this fact does not support their fungibility: Code may indeed be law, but not all code is equal. And understanding the complexities of this connection is profoundly important to understanding the path of cyberlaw.

In a series of seminal works in the late 1990s, several legal academics posited that technology has profound regulatory effects in the online environment.<sup>3</sup> As Lawrence Lessig stated:

---

<sup>1</sup> See, e.g., Lawrence Lessig, *Code and Other Laws of Cyberspace* 6 (1999) [hereinafter *Lessig, Code*]; Lessig, *Law of the Horse: What Cyberlaw Might Teach*, 113 *Harv. L. Rev.* 501 (1999) [hereinafter *Lessig, Horse*]; Ethan Katsh, *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*, 1996 *U. Chi. L. Forum* 335 (1996); Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 *Texas L. Rev.* 553 (1998); James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors* 66 *U. Cin. L. Rev.* 177 (1997). For non-legal treatments, see also William Mitchell, *City of Bits: Space, Place, and the Infobahn* 111 (1995); Andrew Shapiro, *The Control Revolution* (1999).

<sup>2</sup> Tim Wu makes a similar point. See Tim Wu, *When Code Isn't Law*, 89 *Va. L. Rev.* 679, 681-82 (2003).

<sup>3</sup> See, e.g., Lessig, *Code*, supra note 1, at 6; Lessig, *Horse*, supra note 1, at 503; Katsh,

In real space we recognize how law regulates—through constitutions, statutes, and other legal codes. In cyberspace we must understand how code regulates—how the software and hardware that make cyberspace what it is *regulate* cyberspace as it is. As William Mitchell puts it, this code is cyberspace’s ‘law’. Code is law.<sup>4</sup>

This insight into the power and importance of software code in this context has become both broadly accepted and widely discussed.<sup>5</sup> Its implications are disputed: some commentators, most prominently Lessig, suggest that technology—harnessed by commercial interests—is likely to substantially limit freedom in cyberspace;<sup>6</sup> others, (as Tim Wu aptly describes) argue that software code “will arise as a kind of utopian sovereign to improve on perceived failures of state regulation.”<sup>7</sup> Still others, while not disagreeing with the central code-is-law point, inquire as to whether it raises much of an issue at all.<sup>8</sup>

As important as the ongoing debate, however, is what is *not* debated. The idea that code has regulatory effects similar to law is firmly cemented into the consciousness of cyberscholars.<sup>9</sup> And for good reason: it would be an unusually imperceptive internet user who would fail to intuit the behavioral effects of everyday features of cyberspace, such as password requirements, web site registrations, etc. Indeed, the regulatory nature of technology is a point not at all confined to cyberspace; fences are traditional forms of property control, and closing one’s office door clearly regulates the passage of light, sounds, and people.<sup>10</sup> (The concept’s import in cyberspace comes from the uniquely mutable

---

supra note 1, at 340; Reidenberg, supra note 1, at 554; Boyle, supra note 1, at 182.

<sup>4</sup> Code, 6.

<sup>5</sup> See, e.g., Tom W. Bell, *Escape from Copyright: Market Success vs. Statutory Failure in the Protection of Expressive Works*, 69 U. Cin. L. Rev. 741 (2001); Kenneth W. Dam, *Self-Help in the Digital Jungle*, 28 J. Legal Stud. 393 (1999); Wu, supra note 2, at 682; Wu, *When Law & the Internet First Met*, 3 Green Bag 2d 171 (2000); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 Calif. L. Rev. 439, 443 (2003); Orin Kerr, *The Problem of Perspective in Internet Law*, 91 Geo. L.J. 357, 359 (2003).

<sup>6</sup> See, e.g., Lessig, Code, supra note 1, at 6.

<sup>7</sup> Wu, supra note 2, at 683.

<sup>8</sup> See, e.g., Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. Chi. Legal F. 207; Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. Chi. L. Rev. 1199 (1998).

<sup>9</sup> Indeed, a July 2003 search in the LEXIS ALR database using the following query

*"code is law" and (software OR technology OR internet OR cyberspace)*

returned 759 hits.

<sup>10</sup> E.g., Lessig, Code, supra note 1, at 86-90.

nature of the computer technology that forms the online world.)<sup>11</sup> In sum, *Code Is Law* contains an essential truth that is both attractive and impossible to ignore.

Yet there is a way in which this central descriptive principle disserves as well. For *Code is Law* carries with it what might be said to be the implication of equivalence: an unstated premise going to the relationship between “code” and “law.” Specifically, the code-is-law meme at least evokes the idea that software code and legal code are somehow regulatory substitutes. But as should be obvious, this does not necessarily follow, logically or factually: That technology has regulatory impact does not suggest that it is directly interchangeable with law, and it is easy to understand how the regulatory mechanisms differ.<sup>12</sup> Note that this is not to suggest that the pioneers of the code-is-law principle stated as much, or even that they failed to understand this point.<sup>13</sup> Nobody, for example, seems to argue directly that any particular snippet of software can directly substitute for a particular statutory provision. And yet, lurking in the background of much recent work that accepts as true the *Code is Law* proviso is the question of the relationship: how, exactly, does regulation-by-software compare to regulation-by-law, and how do the two interact?

Indeed, the understanding that software code (as well as law) can have regulatory effects itself demands inquiry into the nature of the relationship.<sup>14</sup> For if either software or law can provide a relevant legal infrastructure, then policymakers have a choice. And if software and law regulate in different ways, with different strengths, weaknesses, costs, and benefits, then that choice—regulation-by-software or regulation-by-law—will have crucial implications.<sup>15</sup> Further, in the cyberspace context, law and software will necessarily coexist, so the analysis is not only comparative, but dynamic—a complex, multidimensional question. To no small degree, the answer will (and should) drive the policy decisions that determine the emerging regulatory

---

<sup>11</sup> See Lessig, Horse, supra note 1, at 507.

<sup>12</sup> See id. at 509-510.

<sup>13</sup> Indeed, Lessig in particular importantly presaged this line of analysis, noting that what he called ‘modalities of regulation’ would both compete and interact. See Lessig, Horse, supra note 1, at 508-10. See also Lawrence Lessig and Paul Resnick, Zoning Speech On The Internet: A Legal And Technical Model, 98 Mich. L. Rev. 395 (1999).

<sup>14</sup> Tim Wu has recently (and importantly) asked a similar question, noting that software code can at times be used to avoid or mitigate the effects of legal rules. See generally Wu, supra note 2. As noted below, this observation fits well into the analytic structure derived here. See infra note 34 and accompanying text.

<sup>15</sup> See, e.g., Lessig, Code, supra note 1, at 6-9; Lessig, Horse, supra note 1, at 512.

infrastructure of cyberlaw.<sup>16</sup>

This Article develops an analytic framework for understanding the regulatory environment in the context of law and software. At its core, the approach here is part reminder, part reconceptualization: embracing the basic truth of the regulatory effects of both software and legal code, yet rejecting their equivalence. Instead, the relationship between law and software in cyberspace regulation is conceived as essentially complementary; it is the interface of law and software that establishes the complete regulatory conditions. This law-software interface is defined by a rough equilibrium—a mix of regulatory effects established by a complex (and deeply contextual) mixture of legal effects, technological circumstances, and private cost-benefit analyses. In this complex world, less “law” does not necessarily mean less regulation. Instead, in many cases it will imply greater regulation by software; the net regulatory effects are dependent upon the interactions along the law-software interface.<sup>17</sup> Similarly, changes in the technological (software) environment will advance responsive changes in legal rules, yielding perhaps more or perhaps less regulation, under different circumstances.<sup>18</sup> It is this elemental relationship—between law and software, legal code and software code, lawyers and coders—that provides both the greatest challenge to policymakers in this new frontier of regulation, and the greatest reward for appreciating it.

The understanding of the law-software interface developed in this Article provides a number important insights into the problem of modern regulatory environments. The first is that policy analysis in this context cannot simply consider legal changes; the software-regulatory response must also be considered.<sup>19</sup> Indeed, in many cases, the response may be difficult to predict *ex ante*, meaning that the net regulatory effects are likely to be unclear.<sup>20</sup> Less “law” might result in a greater overall regulatory condition—or simply no effect at all. A second key observation is that dynamism is the rule rather than the exception.<sup>21</sup> Driven by continuing changes in technology, as well as new innovations in models of creating and distributing information, the law-software interface will be under constant pressure. This suggests that regulatory policy

---

<sup>16</sup> See, *id.*

<sup>17</sup> Lessig makes a related point. See, e.g., Lessig, *Code*, *supra* note 1, at 189 (the absence of law “will cause a shift in effective regulatory power - from law to code, from sovereigns to software.”)

<sup>18</sup> See, e.g., Wu, *supra* note 2, at 682.

<sup>19</sup> See *infra* notes 28-35 and accompanying text.

<sup>20</sup> See *infra* notes 50-61 and accompanying text.

<sup>21</sup> See *infra* notes 44-48 and accompanying text.

must search for flexible solutions, and that efforts to codify a ‘current’ understanding of the Internet, for example, are unlikely to succeed.

And yet there is a dark side to the emergence of software code as a regulator. The very features of software that make it a viable (and often attractive) alternative to legal regulation can have troubling public effects, at least as compared to legal regulation.<sup>22</sup> Software regulation lacks forms of regulatory ‘safety valves’—for example, the involvement (even cursory) of third parties, which serves to temper ‘extreme’ arrangements. Software regulation does not generally require evaluation of enforcement costs: marginal costs are near zero. And the scaling effects of software (software ‘regulates’ essentially the same irrespective of amount of use) are quite different from legal regulation. Together, these factors suggest rather strongly that the over-use of software regulation will yield a regulatory environment that is at once more extreme and less stable than that with more participation from law. This in turn suggests that an important criterion for policy analysis in cyberspace is the potentially-large social benefit of more law and less software.<sup>23</sup>

Understanding the law-software interface can also greatly influence the choice of a legal rule-form. Just as simply considering legal options for cyberlaw is deeply incomplete, the choice of legal form here is not simply between the traditional categories of property rules and liability rules.<sup>24</sup> A third form of legal rule—the direct control of software regulatory effects, denoted here as *legal preemption*—must also be considered. In addition to this added axis of evaluation, the insight noted above—the detrimental public effects of software—forces evaluation of legal rule-forms according to both their normative effects (How well does the rule perform overall?) *and* their instrumental effects (How well does the rule form affect the law-software interface?). Adding these factors into the analysis suggests that the key choice in this context is between relatively strong forms of property rules and hybrid

---

<sup>22</sup> Note that this is a different set of concerns about the rise of regulatory software code than those articulated by Lessig. See generally Lessig, *Code*, supra note 1. Lessig’s chief concern relates to *who* controls software code—particularly private, commercially-interested parties, who may not (indeed, likely do not) have the general public interest in mind. See *id.*

The elements of the case against software developed here are inherent in the nature of software-as-regulator, rather than being contingent on the identity of the code writer. See *infra* notes 66-67 and accompanying text. Thus, these concerns hold even where the software code is developed using ‘open source’ methods, which Lessig suggests would moderate his concerns. See, e.g., Lessig, *Code*, supra note 1, at 100-109,

<sup>23</sup> See *infra* notes 66-74 and accompanying text.

<sup>24</sup> See Guido Calabresi & Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 *Harv. L. Rev.* 1089, 1092 (1972).



rules containing forms of legal preemption.<sup>25</sup>

Applying the analytic framework developed here to one of the most complex and controversial regulatory challenges in cyberspace—the question of the appropriate entitlement regime for access to network-connected resources, or *cyberproperty*—confirms its utility as a tool for cyberlaw policy analysis.<sup>26</sup> In stepping through the analytic framework developed by this Article, a possible legal rule for cyberproperty emerges: a hybrid approach of a broad property rule, a default condition in favor of open access, and a form of legal preemption supporting software mechanisms to facilitate notice and/or transactions. More important than the result, however, is the process—the integration of the multifaceted relationship between law and software into analysis of modern regulatory choices.

Considering the regulatory environment of cyberspace from the perspective of the framework of this Article may have profound effects on the way we think about the form and function of law online. Less law does not mean more freedom. The over-reliance on software regulation can have negative social consequences. Flexibility in legal rules is paramount; traditional liability rules appear to be especially unsuited for this environment. And while the case is far from clear (and subject to a number of contextual dependencies), the nature of cyberspace as particularly sensitive to emerging concerns about the tyranny of software suggests that the online environment might be more suited for a broad property rights regime than has been widely recognized. Code is law, but law is better.

---

<sup>25</sup> See *infra* notes 108-111 and accompanying text.

<sup>26</sup> For major cyberproperty-related cases, see, e.g., *Intel, Corp. v Hamidi*, No. S103781 (Cal., June 30, 2003); *eBay, Inc. v Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000); *Thifty-Tel, Inc. v. Bezenek*, 54 Cal. Rptr. 2d 468 (1996); *Compuserve, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997); *Register.com, Inc. v. Verio, Inc.* 126 F. Supp. 2d 238, 249-50 (S.D.N.Y. 2000).

For academic treatments, see, e.g., Richard Epstein, *Cybertrespass*, 70 U. Chi. L. Rev. 73 (2003); David McGowan, *Website Access: The Case for Consent*, \_\_ Loy-Chi. L. J. \_\_ (forthcoming 2003); Trotter Hardy, *The Ancient Doctrine of Trespass to Websites*, 1996 J. Online L. art. 7; Dan L. Burk, *The Trouble With Trespass*, 4 J. Small & Emerging Bus. Law 27 (2000); Nina Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 49 J. copyright Soc'y 165 (2001); Maureen O'Rourke, *Property Rights and Competition on the Internet: In Search of An Appropriate Analogy*, 16 Berkeley Tech. L. J. 561 (2001) [hereinafter O'Rourke, *Analogy*]; Maureen O'Rourke, *Shaping Competition on the Internet; Who Owns Product and Pricing Information?*, 53 Van. L. Rev. 1965 (2000) [hereinafter O'Rourke, *Shaping Competition*].



What follows has four parts, beginning, in Section II, with the outline of the basic analytic framework, establishing the concept of the law-software interface, and exploring the complexities in determining the equilibrium point that will determine the regulatory condition.

Section III builds on this framework by noting the serious concerns inherent in software regulation, suggesting that in many cases a policy goal should be to develop regulatory conditions with more law and less software.

Next, Section IV looks at how the understanding of the law-software interface influences the choice of legal rules, and notes that such an approach is likely to add at least some force to arguments in favor of property rules, in addition to highlighting the importance of rules involving legal preemption.

Section V applies the foregoing analysis to the regulatory environment for access to network connected resources—cyberproperty. The results suggest both that the framework here is viable, and that it might offer additional force to the arguments in favor of modified property rules.

Section VI provides a brief conclusion.

## II THE LAW–SOFTWARE INTERFACE: AN ANALYTIC FRAMEWORK

This section provides a basic analytic framework for thinking about the relationship between the two major regulatory modes of cyberspace noted above, law and software.<sup>27</sup> This construct emerges from the observation that the law-software relationship in cyberspace is primarily defined by complementarity rather than substitutability, fundamentally additive rather than subtractive. Put

---

<sup>27</sup> As Lessig has aptly noted, social norms and the marketplace will each of course have important regulatory effects in cyberspace, as they do in realspace. See Lessig, Horse, *supra* note 1, at 507-10. For simplicity, and because the most interesting interaction for the purposes of the online legal environment exists between law and software, the effects of norms and the market will be noted less systematically, though their most important effects will be described.

more simply, for a given regulatory condition, the impact of law—cases, statutes, etc.—will deeply influence the impact of software. Indeed, the idea here is to think in terms of equilibria, the natural resting point on the law-software interface.

Conceptualizing the relationship between law and software in this manner brings at least two important implications into sharp relief. First, the analysis of policy options in the cyberspace context will necessarily be dynamic in nature, requiring consideration of not only (for example) legal adjustments, but also predicting the responsive effects such changes will stimulate in software regulation. That is, policy arguments, proposals, and critiques in this brave new world will be fundamentally incomplete without careful attention to both legal and software effects, and the integrated relationship between the two.

Second, the rapidly advancing pace of software development and deployment, as well as the resulting instability of any law-software equilibrium conditions, points out the deep-seated challenges inherent in policy development in cyberspace. Indeed, these problems appear to be so fundamental—and particularly acute for certain institutional actors, such as the judiciary—as to suggest that over-reliance on software regulatory techniques as a policy lever will be counterproductive. A close look at the law-software interface might lead to the conclusion that an overarching policy goal for cyberspace might be to build more law—and less software.

#### *A. Code Meets Law*

That software code in the cyberspace context is regulatory in effect is not seriously debated.<sup>28</sup> The more pressing inquiry relates to the nature of the law-software relationship, and its effects on the behavioral infrastructure of cyberspace.<sup>29</sup> The analytic framework developed and explored here is based on the following premises:

- (a) Both legal code and software code have regulatory effects;
- (b) Legal effects and software effects are interrelated—a change in one regulatory mode will affect the other (at least over the medium-to-long term); and
- (c) The total regulatory condition is the product of both legal

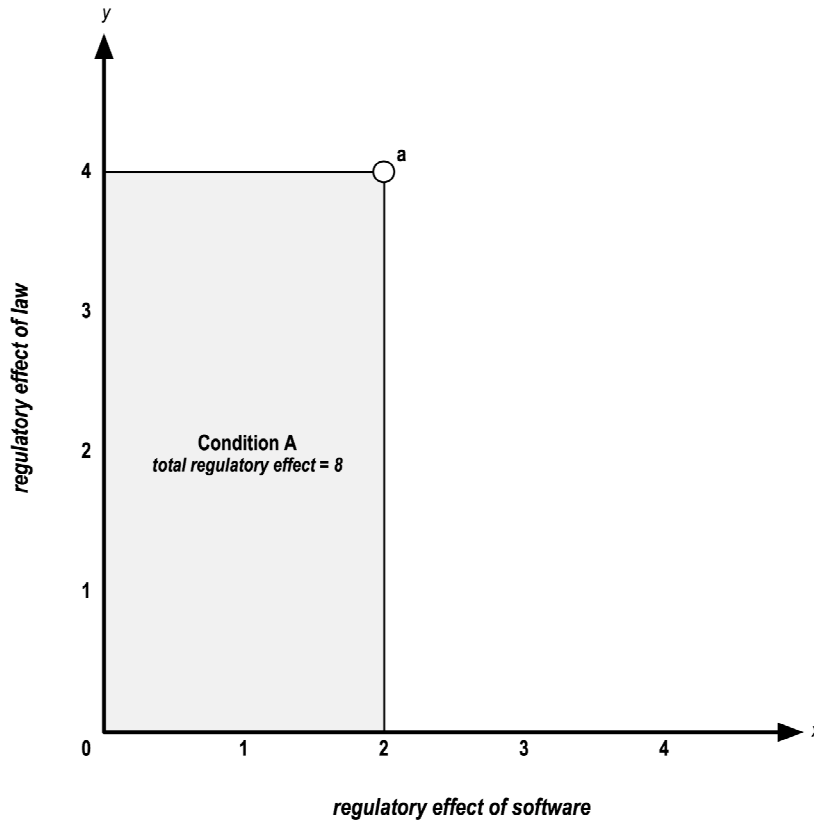
---

<sup>28</sup> Though the normative implications of this are controversial. See *supra* notes 5-8 and accompanying text.

<sup>29</sup> See, e.g., Wu, *supra* note 2, at 679.

regulatory effects and software regulatory effects.

Figure 1, below, depicts the basic point here graphically.



*Figure 1: The Law-Software Interface*

Here, the axes represent the effects (or impact) of the two regulatory modes, law (y-axis) and software (x-axis).<sup>30</sup> A greater “regulatory effect” means a greater impact on behavior; for example in a paradigmatic property-rights case, greater regulatory effect means greater protection to property owners. The total regulatory effect is the area defined by the law-software interface. Consider regulatory Condition A above, with a given legal impact (here, 4), and a software effect (here, 2). In the

---

<sup>30</sup> Again, to be complete the Figure should encompass four dimensions, corresponding to each of law, software, norms, and the market as having regulatory effects. See, e.g., Lessig, Code, *supra* note 1, at 52-54. The author, however, found it problematic to graphically describe the more encompassing relationship.

Figure 1 construct, the equilibrium condition is depicted as point *a* (2,4), and the total regulatory effect is designated as  $2 \times 4 = 8$ .

Less abstractly, and using the cyberproperty example central to this paper, regulatory Condition A can be said to represent the total excludability that owners of Internet-connected resources (web servers, email systems, etc.) enjoy—that is, the content of the “cyberproperty” right. That quantum of regulatory effect (again, designated as 8 here) is the product of *both* legal protections—perhaps state-backed property-type rights (doctrinally, a remedy for trespass)<sup>31</sup>, *and* software-constructed protections, such as link-denial code, password protections, or others.<sup>32</sup>

Another useful example is copyright. In this context, Condition A in Figure 1 represents the total appropriability provided to the creator of an expressive intellectual good: the “copyright”. The legal regulatory effects are established by the protections and limitations of Title 17 of the United States Code.<sup>33</sup> The technological effects include both the availability of protection-enhancing software, such as Digital Rights Management (DRM), as well as the existence of what Tim Wu describes as “anti-regulatory” code—software that undermines the appropriability of the work.<sup>34</sup> This example (in both its dimensions) illustrates that the impact of both law and software must be considered *on a net basis*. Just as software in the digital media context (to give one example) has both pro-protection and anti-protection effects, the Copyright Act both provides legal protections and sets legal limits.<sup>35</sup> What is important for establishing the equilibrium, and thus total appropriation, is the net effects of each regulatory system, law and software.

### *B. Equilibrium at the Law-Software Interface*

Having established the basic terms of Figure 1—what is meant by the law-

---

<sup>31</sup> As I note in the discussion in Section V below, the uncertainty associated with the existence, scope, and nature of the legal protections for the “cyberproperty” right has important policy consequences.

<sup>32</sup> See *infra* Section V below for a detailed look at the software-regulatory options.

<sup>33</sup> See generally 17 U.S.C. § 106.

<sup>34</sup> The canonical example, and the one discussed in detail by Wu, is peer-to-peer software products, which allow for easy—and only partially regulable—exchange of copyrighted goods (typically music or movies) between network users. Wu, *supra* note 2, at 700-02.

<sup>35</sup> Compare 17 U.S.C. § 106 with 17 U.S.C. § 107.

software equilibrium—it next becomes crucial to understand the response mechanisms that produce this condition. One important point here is that the responses can be expected to flow in *both* directions: legal conditions will provoke a technological response, and technological circumstances can prompt legal changes. In cyberspace, neither legal nor software code exists in a vacuum; their tight coexistence creates a continual feedback loop.

Note that the equilibrium-response posited here, for both law and software, is driven by private cost-benefit considerations.<sup>36</sup> There are of course tremendously important *public* effects and responses, as discussed in Section III below; the point of the analytic framework here is to describe the impact of private decision-making on the regulatory environment.

Put most directly, equilibrium at the law-software interface is determined by the contextual cost-benefit functions of the law and software regulatory mechanisms. For example, given a legal regulatory condition, greater software regulation will be deployed (moving the equilibrium point to the *right* in

Figure 1 above) where it is cost-effective to do so, where the gains outweigh the costs. Again, consider the cyberproperty example. Absent any technology effects, a web site owner will have a certain level of legal protections against unwanted use of her network resources: certainly protections against outright hacking, perhaps protections based on unauthorized access as a form of trespass, perhaps rights established by a Terms of Service (TOS) contract with users, and maybe rights emanating from copyright law. Each of these legal rights and remedies of course has related costs and difficulties, most prominently the costs of enforcement, but also costs related to effectiveness—for example, as generally *ex post* mechanisms, they trigger themselves only after a violation arises, which may offer less protection in the dynamic Internet environment.<sup>37</sup> Accounting for both the *de jure* protections and their limits based on costs and effectiveness yields a *de facto* (or net) level of *legal* regulatory effect.

Evaluating this net legal impact presents the web site owner with a choice concerning whether to deploy software-based regulatory mechanisms. For

---

<sup>36</sup> They also represent average behavior. Obviously, in the absence of explicit restrictions otherwise, see *infra* text accompanying note 46, individual responses to legal effects will vary. The Figures here are intended to convey the overall overage response rather than suggest that all players will behave the same.

<sup>37</sup> For example, if the harm the web site operator suffered as a result of an unwanted link was a sudden rush of traffic that exceeded the capacity of the web server, either causing a crash that resulted in at least temporary downtime or greatly slowing access to the site, an *ex post* remedy would seem pyrrhic; though if monetary damages could be calculated, in theory they might be recovered. Similarly, the possibility of an injunction against future unwanted links might be useful in some cases.

example she could implement a link-blocking mechanism based on the http protocol that is intended to allow traffic only from designated referring web pages.<sup>38</sup> The use of this technique will of course increase the level of protection against unwanted use of network resources, though it obviously comes with a series of related costs, both monetary and otherwise.<sup>39</sup> Ultimately, deployment will depend upon the net software effects—the gains to be had from additional software regulation—given the extant legal protection. Thus, under this example, the location of point *a* in

Figure 1 is a function of these calculations. Again, this is the central lesson of cyberlaw: regulatory effect (here, total protection) is the product of law and software.<sup>40</sup>

Note also that the response-effects do not flow in only one direction. Technological circumstances can drive legal changes. Consider the radical shifts in the environment surrounding the music industry:<sup>41</sup> These changes, ranging from the advent of digital media to the development of peer-to-peer file sharing software, have led the industry to seek (at times successfully)<sup>42</sup> stronger legal regulations, as well as yielded new litigation tactics calculated to increase the net effects of the copyright law.<sup>43</sup> Again in Figure 1 terms, this moves point *a* *upwards*, indicating a greater legal regulatory effect—and thus greater overall regulatory conditions, assuming stable software effects.

---

<sup>38</sup> I call this the *http-referrer* blocking technique. I discuss this and many other software regulatory effects in Section V below.

<sup>39</sup> As discussed at length in Section III below, a major cost of technological mechanisms in the cyberproperty context, given the current state of the technology, is their inflexibility. A *http-referrer* blocking technique offers a binary choice (block or no block), rather than the more nuanced conditional blocking (block unless conditions *x*, *y*, and *z* are satisfied) that might be more satisfactory to many web site operators. Another cost is that http-referrer mechanisms are not too difficult to evade.

<sup>40</sup> See *supra* note 1 (collecting sources).

<sup>41</sup> See, e.g., Stanley A. Miller II, *Peer-to-Peer Networks Are Here to Stay*, MILWAUKEE J. SENTINEL, Mar. 25, 2003, at 4E, available at 2003 WL 3313281; Anna Wilde Mathews, Martin Peers & Nick Wingfield, *Off-Key: The Music Industry is Finally Online, But Few Listen*, WALL ST. J., May 7, 2002, at A1, available at 2002 WL-WSJ 3393936.

<sup>42</sup> See, e.g., 17 U.S.C. § 1201 (2002) (DMCA).

<sup>43</sup> Lisa M. Bowman and Evan Hansen, Verizon to hand names over to RIAA, CNET News.com, June 4, 2003, 4:44 PM PT, <http://news.com.com/2100-1025-1013154.html>. Note that the record industry is pursuing a variety of fronts, including normative and technological.

*C. Implications of Code Meets Law I: Dynamic Effects*

Setting out this basic framework—understanding that regulatory conditions are determined by the complementary effects of both law and software, and that the intricate relationship between law and software is critical to the location of the equilibrium point—leads to a number of important observations and implications. Perhaps the most important, and most straightforward, of these observations is that the law-software interface is profoundly dynamic in the cyberspace context.<sup>44</sup> That conditions change, of course, is unremarkable. What makes the dynamic effects of the cyberspace regulatory environment noteworthy is the interrelationship between the two regulatory modes: as described above, the complementary relationship implies that changes along one dimension will (certainly over the longer term) yield changes in the other.<sup>45</sup> From a policy perspective, this observation is crucially important: it means that policy adjustments in the cyberspace context cannot merely be contemplated as one-dimensional changes (paradigmatically to legal scholars, changes in the legal environment). Instead, a complete policy proposal or analysis in this arena cannot afford to overlook the dynamics of the law-software relationship. That is, a proposal for legal change is incomplete without predictions concerning the software response to such a change: for, as noted above, it is the product of law and software effects that determine the overall regulatory environment.

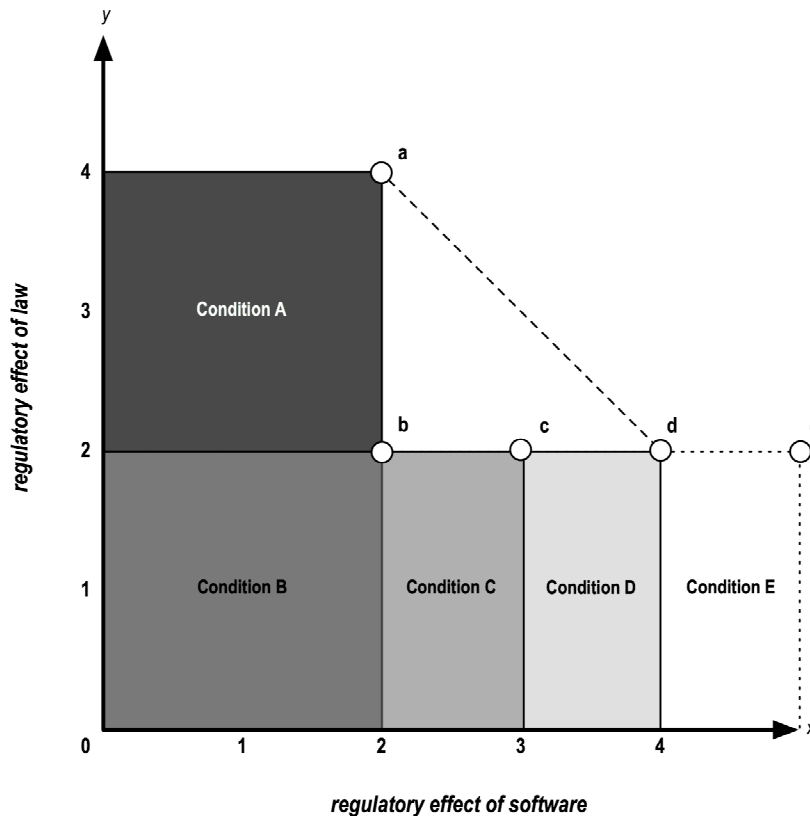
Consider, for example, Figure 2, depicting changes in conditions.

---

<sup>44</sup> Indeed, this dynamism—driven primarily by technological (software) changes—is fundamentally why the relationship between law and technology is so evidently important in this area of the law, while it garners relatively less attention in other areas.

<sup>45</sup> Obviously, there are quite likely to be short-term effects where the response to changes in one regulatory mode are small to nonexistent. Given the nature of the legislative and judicial system, one can expect these transitional effects to have more significance in slowing legal changes in response to software developments than vice-versa.





*Figure 2*

Figure 2 describes a change in legal regulatory effects (a decrease from 4 to 2; for example, the reduction or elimination of a cyberproperty right), and explores the implications of various technological responses. Points b, c, d, and e describe a range of possible software responses, each yielding a very different overall regulatory environment. Condition B is the case where there are no long-term software effects; perhaps because of the high cost of the software regulatory mode (for example, it might be the case that the appropriate software does not meaningfully exist, or is impossibly inflexible to be useful).<sup>46</sup> In this case, total regulatory effect reduces from an 8 in Condition A (2 x 4) to a 4 in Condition B (2 x 2). Given a utilitarian model, one would thus expect a change in output or development of the protected/regulated good in Condition B. This could be either a positive or negative change, depending upon a variety of assumptions about the development environment; for purposes of the illustration

---

<sup>46</sup> Another possibility for Condition B, which I discuss more fully below, see *infra* notes 86-95 and accompanying text, is that the legal regulation directly implicates the software regulation, perhaps by preempting or discouraging certain software deployments.

here, the direction and magnitude of the output-effects are unimportant.

Condition C in Figure 2 describes the circumstance where software effects increase *somewhat* in response to the decreasing legal regulatory effects. For example, the reduction of the legal cyberproperty right might yield an increased reliance on link-blocking software, such as *http-referrers*. This increase in software effects, however, does not make up for the reduced legal effects, and the overall regulatory effects drop to 6 (3 x 2). Again, one should expect a change in output/development.

Condition D illustrates an increase in software effects of a magnitude that renders no net change in regulatory environment. Here, law and software are fungible, at least from a net regulatory effects perspective. (As discussed in Part D. below, they are clearly not truly fungible even in this case, and there are good reasons to believe a shift in the direction of additional software might be socially harmful.) There should be little, if any change in overall output in the shift from Condition A to Condition D.

Condition E describes an unlikely—but not implausible—scenario: where the reduction in legal effects prompts a technological response of such a dimension that it actually increases the overall regulatory effect. This could occur, for example, if the increase in resources devoted to research and development of software regulatory techniques (spurred by the drop in legal effects) yielded a sort of cost-effectiveness breakthrough, allowing greatly increased deployment of software mechanisms. Perhaps a reduction in the legal force of Copyright law spurred research and development (R&D) into DRM systems that enabled huge advances in effectiveness to be made.<sup>47</sup> Condition E could also occur where cost-effective software responses were profoundly inflexible, essentially ‘forcing’ deployment of more effective protections. An example here might be the reduction or elimination of the cyberproperty right, resulting in dramatically-increased use of password-protected (or otherwise individually-restricted) network resources.<sup>48</sup> Given the change in overall regulatory effect (an increase to 10 (5 x 2)) Condition E will also feature output/development effects, in the opposite direction from those resulting from Conditions B and C.

---

<sup>47</sup> Say, for example, “unbreakable” DRM systems, or even copy-protected CDs that worked reliably.

<sup>48</sup> Note of course that greater total protection (regulatory effects) is not necessarily in the interest of the owner of the protected good (nor, of course, of society generally). If the technology landscape was such that web site owners who wished to prevent unwanted access were required to use the relatively blunt instrument password systems—and that because of the costs of unwanted access, this was cost-effective—greater protection might indeed be suboptimal for all concerned.

The point of working through each of the Conditions in Figure 2 is to illustrate the critical attention that must be paid to the law-software interface in the cyberspace context. Legal-policy proposals unsupported by predictions of technological response are deeply incomplete. Without an understanding of whether the software response point will be *b*, *c*, *d*, or *e*, the best-laid policy plans seem likely to go awry. For example, if a policy goal was to reduce the overall regulatory effect in a particular context—perhaps to support wider web linking by decreasing legal protection for network resources, or perhaps to broaden re-use of copyrighted materials by expanding the notion of fair use—a proponent would undoubtedly be quite disappointed to find that the reduction in legal effects had resulted in no overall regulatory effects (Condition D in Figure 2) or had actually *increased* protection (Condition E in Figure 2). Indeed, even an unexpected difference in end-state regulatory effects (say, between Condition B and Condition C) could derail carefully-calibrated policy initiatives. The intertwined relationship between law and software demands careful consideration of each. Code is not equivalent to law, and it matters crucially in cyberspace.

#### *D. Implications of Code Meets Law II: Unpredictability & Uncertainty*

Having established the importance of analyzing the law-software relationship to the regulatory content of cyberspace, the great difficulty of doing so can now be explored. The following sections explores two distinct-but-related points. First, predicting the software response to changes in the legal environment is likely to be quite difficult in all cases, and especially difficult for judicial actors, who are generally neither trained in software analysis, nor likely to receive complete information concerning the range of possible software effects to legal decisions. Second, given the rapid development of software technologies (especially in the cyberspace context) in recent years, any “steady-state” equilibrium point (such as those depicted in Figures 1 and 2 above) would appear to be fleeting, suggesting that analysis-based policymaking in cyberspace requires hitting a moving target. Taken together, these points begin to make the case that the overuse of software (or other technologies) as a policy lever could be counterproductive.

##### 1. Unpredictability

Perhaps no industry in recent memory has progressed as far and as fast as the

software industry, burgeoning into a \$245 billion business by the year 2000.<sup>49</sup> Further, given the continuing rapid rate of increase in computer processing power, it seems clear that the depth and breadth of software development will continue unchecked for the foreseeable future.<sup>50</sup>

This rapid, and perhaps even accelerating, pace of innovation (and, more significantly for purposes here, deployment) has important implications for the regulation of cyberspace. Applications that seemed fanciful mere years ago, such as television-on-demand,<sup>51</sup> or seamless (and borderless) data file transfer,<sup>52</sup> are now commonplace. The costs (and complexity) of publishing oneself in cyberspace has plummeted rapidly.<sup>53</sup> And yet still one gets the sense that only the tip of the iceberg is yet showing.

Larry Lessig has powerfully argued that the spreading ubiquity in software is not unreservedly a good thing, in major part because its most powerful developers are generally commercially-motivated, and thus predictably place myopic commercial interests ahead of the greater good.<sup>54</sup> The argument here, however, is that perhaps the *unpredictability* of software development and deployment—uncertainties about the rate and direction of ongoing innovation—places an even greater challenge in front of legal development in

---

<sup>49</sup> See, e.g., US Census Bureau, Statistical Abstract of the United States 565 (2000) (Communications & Information Technology).

<sup>50</sup> See, e.g., Martin Campbell-Kelly, From Airline Reservations to Sonic the Hedgehog: A History of the Software Industry 303-05 (2003).

Advances in computer technology are driven in large part by the continuing applicability of Moore's Law, which posits that the density of transistors in semiconductor manufacturing (and thus the underlying processing power available) will double approximately every eighteen months. This observation has more or less held true since it was first noted in 1965 (although Moore's original prediction was actually a slightly more optimistic doubling every year.) See, e.g., Gordon Moore, Cramming More Components into Integrated Circuits, 38.8 Electronics (April 19, 1965); John Markoff, *Is There Life After Silicon Valley's Fast Lane?*, N.Y. TIMES, Apr. 09, 2003, at C1. Moore has recently suggested that the 'Law' is likely to continue for some period into the future. See Gordon Moore, No Exponential is Forever ... but We Can Delay 'Forever', Presentation at International Solid State Circuits Conference (ISSCC) February 10, 2003, available at [ftp://download.intel.com/research/silicon/Gordon\\_Moore\\_ISSCC\\_021003.pdf](ftp://download.intel.com/research/silicon/Gordon_Moore_ISSCC_021003.pdf).

<sup>51</sup> See, e.g., Seth Schiesel, Video on Demand Is Finally Taking Hold, N.Y. Times, Nov. 25, 2002 p. C4; Peter Grant, Miss the Final 'Sopranos'? Getting Cable TV on Demand, Wall. St. J., Dec. 12, 2002, p. D1.

<sup>52</sup> See Wu, *supra* note 2, at 132–135 (describing peer-to-peer software technologies)

<sup>53</sup> See, e.g., Weblogs.

<sup>54</sup> See Lessig, Code, *supra* note 1, at 6.

cyberspace.<sup>55</sup> Software is a constantly-updated regulatory mode; if simply keeping up is a nontrivial exercise, making meaningful predictions presents an even greater challenge.

The line of reasoning here is straightforward. As with many innovation processes, software development is both cumulative—building on what has already been done<sup>56</sup>—and revolutionary—moving in sudden ‘leaps ahead.’<sup>57</sup> The result is a trendline that advances in alternate periods of steady progress and paradigm-busting hurdles. Even identifying which phase presently exists is a challenge: for example, the primary author of the original web browser recently decried the end of innovation on the world-wide-web.<sup>58</sup> And yet the last several months have shown an explosion of activity surrounding web logs (or blogs) as an innovative medium of communications,<sup>59</sup> as well as the advent of apparently-viable web-based models of music distribution.<sup>60</sup> Similarly, does the music industry’s recent focus on litigation and legislation (both legal, rather than software, effects) imply a ‘slow period’ in the implementation of DRM, or are major advances being made behind the scenes? Further, consider that much software technology exhibits network effects, which leads to dramatic increases in impact once a critical level of adoption or deployment is reached.

---

<sup>55</sup> See, e.g., Campbell-Kelly, *supra* note 50, at 305-06.

<sup>56</sup> See, for example, the long-term development of UNIX-type operating systems, now spanning four decades. See generally Peter H. Salus, *A Quarter Century of UNIX* (1994); Lucent Techs., *The Creation of the UNIX Operating System*, at <http://www.bell-labs.com/history/unix/>; Apple Computer, *The Open Desktop*, at <http://www.apple.com/macosx/technologies/darwin.html> (describing the UNIX underpinnings of its most modern operating system, Mac OS X).

<sup>57</sup> The paradigmatic example here is the 1990s explosion in software development surrounding the World-Wide-Web and other networking technologies. See, e.g., Tim Berners-Lee, *Information Management: A Proposal*, March 1989, at <http://www.w3.org/History/1989/proposal.html> (proposing the World-Wide-Web system); World-Wide-Web Consortium (W3C), *A Brief History of the World-Wide-Web*, at <http://www.w3.org/History.html>

<sup>58</sup> Bernhard Warner, *Netscape Founder Says Web Browsing Innovation Dead*, Reuters, July 1, 2003.

<sup>59</sup> See, e.g., Matthew Rose and Christopher Cooper, *Web Logs: Troops' War Stories in Real Time*, *Wall St. J.*, March 25, 2003, at B1; Noah Shachtman, *With Incessant Postings, a Pundit Stirs the Pot*, *The New York Times*, January 16, 2003, p. G5.

<sup>60</sup> See, e.g., Sarah McBride, *Virgin Group Plans New Venture to Enter Online Music Business*, *WALL ST. J.*, March 8, 2004, at B4 (online music sales estimated at \$200 million), available at 2004 WL-WSJ 56922173. *But see* John Markoff, *New Economy; Apple's Success with iPod May Presage the Ascendance of Hardware over Software*, *N.Y. TIMES*, Jan. 19, 2004 (“Apple makes little or no profit from each song downloaded, [but sales of digital music players] were crucial to Apple's financial resurgence.”)

That the unpredictably rapid nature of software development poses great challenges for policy analysis in cyberspace seems quite clear, given its important regulatory effects. But perhaps even more critically, this unpredictability would seem to pose especially acute problems for judicial actors, who are both quite unlikely to have personal skills related to software development and seem far less likely than legislatures to have the resources to become more informed.<sup>61</sup> This in turn argues that leaving important cyberspace policy decisions in the hands of judges is unlikely to be productive.

## 2. Instability

Another major concern related to software regulation is instability. As demonstrated above, cyberspace regulation is the product of legal and software effects; the key analytic factor is the location of the law-software equilibrium point. And yet, given the rapid developments in software technology, the stability of such equilibria would appear to be quite temporary.<sup>62</sup> For example, only relatively minor forms of DRM seem to exist presently in the music context<sup>63</sup>; one could argue that an equilibrium has been reached, an accommodation between consumers, commonly-available technology, and the music creators. But technological advancement could upset this balance, resulting in greater regulatory effects in the future.<sup>64</sup> Indeed, one might expect that the ongoing process of software development and deployment in the cyberspace context would tend to increase software effects (and thus overall regulatory effects) over time.<sup>65</sup> These instability effects again suggest that over-reliance on software as a significant component of the regulatory infrastructure is likely to be problematic.

This section has established an analytic framework for the interrelated regulatory effects of legal and software code, emphasizing both the complex and

---

<sup>61</sup> See, e.g., McGowan, *supra* note 26, at 15.

<sup>62</sup> Absent direct (legal) regulation of software effects

<sup>63</sup> See, e.g., Ethan Smith, *Can Copyright Be Saved? New Ideas to Make Intellectual Property Work in the Digital Age*, WALL ST. J., Oct. 20, 2003, at R1, available at 2003 WL-WSJ 3983145.

<sup>64</sup> See, e.g., Steve Pain, *MS May Have the Answer to Piracy*, BIRMINGHAM POST, Jan. 28, 2003, at P21, available at 2003 WL 7480778 .

<sup>65</sup> Lessig appears to share this concern as well. See, e.g. Lessig, Horse, *supra* note 1, at 529.

contextual nature of this relationship. The remaining sections, below, apply this framework to explore both the public effects of software regulation, as well as its insights into the current controversies over cyberproperty rights.

### III THE CASE AGAINST SOFTWARE: THE PUBLIC EFFECTS OF SOFTWARE REGULATION

If the analytic framework above has made anything clear, it has demonstrated that policy initiatives in cyberspace demand consideration of both legal and software effects. That is, if both law and software are regulatory (and they unambiguously are), and the status of each determines overall regulatory effects, then an important consideration in any policy analysis is the mixture between law and software. It is unquestionable that law and software regulate in different ways; this of course implies that each has different public effects. This section explores the public effects of regulation by software, informing the detailed policy analysis required in the cyberspace context.

The picture of public software effects that emerges is troubling, bringing into sharp relief a number of important concerns about software-based regulation. Note that these concerns are quite distinct from those identified by Lessig in *Code and Other Law of Cyberspace*: while Lessig was essentially concerned with the identity and motivations of software developers, and the potential for such developers to undermine important legal-policy values,<sup>66</sup> this analysis focuses squarely on the nature of software as a regulatory mechanism. For even if one trusts the way regulatory software is developed and deployed, the fact remains that it sharply differs from law as a mechanism of regulation.<sup>67</sup>

At least some of these differences suggest that, irrespective of the cost-effectiveness calculations explained in connection to Figures 1 and 2 above, software-as-regulator might have detrimental public effects. That is, even if software is an effective regulator under particular circumstances, important public considerations might caution against its overuse. This concern stems from the nature of software as a regulatory mechanism, especially as compared to more traditional legal mechanisms. The most important differential features include the following:

*Preprogrammed.* Software regulation operates in a relatively fixed, rigid

---

<sup>66</sup> See, e.g., Lessig, *Code*, supra note 1.

<sup>67</sup> For example, Lessig appears far less concerned about the spread of open-source developed software code, as it attenuates the ability of private commercial actors (or, indeed, the government) to meaningfully control it. See *id.* at 100-109. See also Lessig, *Horse*, supra note 1, at 536-539



fashion to determine regulatory outcomes. The programmed algorithm is followed without deviation; circumstances outside the scope of the programmer's imagination, for example, are not considered. For instance, a http-referrer link blocking mechanism will block (or allow) designated linking users, irrespective of various exogenous factors—such as motivation, willingness to pay for access, and the like.

*Narrow range of inputs.* Software regulatory mechanisms use a predetermined—and typically relatively narrow—range of inputs in implementing the regulatory rules. Importantly, the quantity, scope and nature of these inputs are often significantly constrained: by the creativity of the programmer, the complexity or sophistication of the software itself, or the environment in which it operates. For example the *http* protocol, which forms the basis of web-based communications, has a relatively small number of fields (headers) that offer information about users that would allow for determinations to be made concerning the authorized use of the network resources.<sup>68</sup>

*Self-contained.* The point here is obvious: Software-implemented regulations are free-standing mechanisms,<sup>69</sup> and do not generally require recourse to other institutional players for enforcement, rules-determination, etc. (Contrast this with more typical legal regulation, which generally requires recourse to other institutions or players—courts, arbitrators, prosecutors, regulatory bodies—for decision-making related to enforcement.)

*Marginally costless.* Software regulatory operations are generally unaffected by the quantity of use.<sup>70</sup> A well-designed authentication or link-blocking system will be able to block a single unwanted request a week, or several per second, without a substantial difference in performance effects.

Taken together, these features of software regulation may look like just that—*features*. Software offers a reliable, unwavering, relatively simple, and at least potentially inexpensive means to implement regulations. But this view of software depends upon one's perspective; mapping a broader, public-oriented

---

<sup>68</sup> Most important among these are the *referer* (sic) header (which passes information concerning the location of the link from which the visitor has traveled), as well as headers directed to authentication (which would only have relevance if the web site was implementing a password-access system or the like). Note also that the web server would inherently know the network address of the requesting user. As described in additional detail below, however, there are relatively simple means to obscure such information.

<sup>69</sup> This is not to say that software regulation won't access external resources, such as databases, for information or assistance; rather, the observation is that software mechanisms inherently combine information-collection, rules-analysis, and enforcement.

<sup>70</sup> At least to a point: there are of course capacity constraints in any system, the violation of which can trigger a number of problems.

view of software regulation reveals a darker side, one that should give pause to proponents of software. The following sections briefly note these implications.

### *A. Software and Regulatory Safety Valves*

Even under legal schemes that demand little-to-no intervention on the part of third-party regulatory institutions (property-backed contracts is the paradigmatic case here) there nonetheless exist a number of what might be called ‘safety valves’ that serve to ensure that otherwise private arrangements conform to acknowledged boundaries of social practice. These safety valves can be explicit: such as unconscionability in contracts (which serves to ensure that agreements are entered into voluntarily), competition law (which serves to ensure that private dealings do not stifle the market’s functioning), or even broader social values, such as antidiscrimination principles. Or they can be less formal, such as the restraint that is encouraged by the knowledge that enforcement of onerous contract terms, for example, will often take place in the public sphere—and thus subject the author to unwanted publicity.

By obviating the need to seek recourse to third party enforcement institutions—such as courts or regulators—software regulation can, to a significant degree, “fly under the radar,” avoiding the oversight, both formal and informal, that occurs even in the *least* interventionist forms of legal regulation (such as property-backed contractual relationships). This in turn implies that the typical forces that, in effect, tend to normalize what otherwise appear to be purely private dealings, will have substantially less impact where software is concerned. There are at least two observations that flow from this recognition. The first is obvious: to the extent that these external constraints on behavior are highly valued, software then becomes a less attractive regulator. The second is somewhat more subtle: increased software regulation increases the incidence of ‘outlier’ regulatory techniques—i.e., those that are beyond the range of social practices. (An example might be an access-blocking mechanism that discriminated on the basis of operating system, so as to leverage control from one market—the web site—to another—operating systems, or one that blocked users affiliated with particular political views.) Such outlier techniques might be expected to destabilize the regulatory environment altogether: on the one hand, it would almost certainly spur further work on anti-regulatory software, thus leading to greater instability in the law-software interface; on the other, it might demoralize the user community to a degree that resulted in socially-detrimental decreases in activity (e.g. web surfing).

### *B. Software and the Recognition of Enforcement Costs*

It is axiomatic that the enforcement of legal rights won't occur where the enforcement costs outweigh the expected gains. While enforcement costs are often viewed as a social drag, their function of allowing for some (low-level) violations of rights can in many cases be beneficial. Hence the concept of "efficient breach" in contract law. This effect of enforcement costs is especially well-understood in the area of intellectual property, where allowing the broadest possible dissemination of intellectual creations—consistent with maintaining appropriate development incentives—is a core value.

In the software regulation context, marginal enforcement costs are essentially zero. Thus, one can predict with confidence that enforcement costs will not be accounted for—they don't exist—and the effects noted above will not be realized. Again, two implications seem especially relevant. The first is the loss of the beneficial effects of the recognition of enforcement costs, noted above. The second is the expectation that the absence of the tempering effect of enforcement costs will result in more 'outlier' regulatory approaches, with similar instability and demoralization potential as with the absence of the safety valves.

### *C. Scaling Software*

As a general matter, software scales well—its behavioral features remain unchanged as the quantity of activity increases. As a regulatory mechanism, this might appear quite attractive; a common problem in legal regulation is overloading of the institutions that provide the regulatory functions. And yet, the scaling features of software may have potentially-troubling public effects as well. For one thing, software regulation is likely to become increasingly vulnerable to countermeasures as the scale of its use increases<sup>71</sup>; it is well-established that popular or widely-used software most encourages the sort of research that would either reveal latent bugs in the software, or develop effective

---

<sup>71</sup> This situation is exacerbated by an institutional tendency to under-report potential defects at the performance-testing stage prior to release. See, e.g., Lisa Liberty Becker, *Telling the Truth Can Be Hazardous to Your Job*, BOSTON GLOBE, Apr. 6, 2003, at G9, available at 2003 WL 3389786; H. Jeff Smith & Mark Keil, *The Reluctance to Report Bad News on Troubled Software Projects: A Theoretical Model*, 13 Info. Systems J. 69 (2003). See generally NAT'L INST. OF STANDARDS AND TECH., U.S. DEPT. OF COMMERCE, THE ECONOMIC IMPACTS OF INADEQUATE INFRASTRUCTURE FOR SOFTWARE TESTING (May 2002).

countermeasures.<sup>72</sup> And software regulation is unlikely to fail gracefully: once bugs or countermeasures are discovered, the effectiveness of the particular regulatory mechanism is substantially diminished.<sup>73</sup> This phenomena—that software becomes increasingly vulnerable to sudden (even catastrophic) failure as its scale increases—again suggests that software is an unstable regulatory device.

Other implications of the scaling features of software are similar to those noted with respect to safety valves and enforcement costs: the loss of a tempering effect that serves to diminish the incidence of outlier or ‘extreme’ private regulatory forms (i.e., terms in contractual relationships). If the costs of a regulatory choice—a particular contract term—increased with scale, one might expect this fact to tend to ‘smooth out’ terms that disproportionately generated controversy or, more significantly, enforcement costs. Including a contractual term requiring users to avoid criticizing the web site owner, for example, might simply cause more trouble than it’s worth, especially as the number of agreements rises rapidly.<sup>74</sup> But in the software regulation context, the ability of software to scale “well” means that these potentially-beneficial scaling effects are absent.

Taken together, the pattern of public-related concerns about software

---

<sup>72</sup> See, e.g., Christopher Jones, *Internet Hacking for Dummies*, WIRED MAGAZINE (Feb. 20, 1998), available at <http://www.wired.com/news/technology/0,1282,10459,00.html>.

Eric Raymond famously made a similar point in the context of the open source movement, noting that “[g]iven enough eyeballs, all bugs are shallow.” Eric Raymond, *The Cathedral and the Bazaar*, in *THE CATHEDRAL AND THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY* 19, 30 (2001). See also Yochai Benkler, *Coase's Penguin, Or, Linux and the Nature of the Firm*, 112 *Yale L.J.* 369, 434-36 (2002).

<sup>73</sup> See, e.g., *Building a Better Bug Trap*, *THE ECONOMIST*, June 21, 2003, available at 2003 WL 5852981; Dan Verton, *Tech Consortium Created to Improve Software Reliability*, *COMPUTERWORLD*, May 20, 2002, at 12. See generally NAT’L INST. OF STANDARDS AND TECH., supra note 71.

Additionally, efforts to repair vulnerable or defective software systems are typically problematic. See, e.g., Douglas Schweitzer, *Emerging Technology: Patch Management—Patch Me If You Can!*, *NETWORK MAG.* (Aug. 1, 2003) (software patches are generally expensive to install on large networks, frequently get released with minimal testing, and often have unintended consequences—such as causing other programs to crash), available at 2003 WL 5398725; George V. Hulme, *Companies Pay Up to Plug Holes*, *INFORMATIONWEEK* (May 20, 2002) (hackers outpace the repair efforts of security administrators), at <http://www.informationweek.com/story/showArticle.jhtml?articleID=6502382>.

<sup>74</sup> See, e.g., Ed Foster, *A Punitive Puppeteer?*, *INFOWORLD* (Sept. 14, 2001), at <http://archive.infoworld.com/articles/op/xml/01/09/17/010917opfoster.xml>

regulation suggests that, as compared to more traditional legal regulatory mechanisms, software is likely to be considerably less stable, as well as contain a higher incidence of “outlier” or “extreme” rules. These concerns need to be factored into any policy analysis in cyberspace, and suggest that software regulation may be considerably less attractive than it might otherwise appear. This is not to suggest that software regulation should be excised as a policy option: indeed, this would seem next to impossible in the cyberspace context. Instead, this argues for a more nuanced view of the trade-offs between legal code and software code.

#### IV

#### SOFTWARE AND THE CHOICE OF LEGAL RULES

The preceding two Sections have demonstrated both the importance of understanding the law-software relationship in the cyberspace context, and how the very different ways that law and software regulate may argue rather forcefully in favor of predominantly legal rather than software-based regulatory approaches. In essence, a better law-software equilibrium is likely to have more law and less software.

This Section explores the implications of the foregoing analysis for the selection of forms of legal rules in cyberspace. That is, proceeding from the premise that the most convenient policy lever available to affect regulatory conditions in cyberspace is law, rather than software, the analysis now turns to the way that the choice of legal rule is influenced by considerations of the law-software equilibrium.<sup>75</sup>

A key observation here is that the choice of legal rules in cyberspace is not just an argument between the classic dichotomy of “property rules” and “liability rules” (and mixtures thereof) but also between traditional legal forms and those that directly impact the scope and quantity of software regulation—forms of legal rules denoted here as *legal preemption*.<sup>76</sup> That is, given the analysis in

---

<sup>75</sup> As Tim Wu importantly suggests, some groups may find software to be a more convenient approach to altering the regulatory landscape. See generally Wu, *supra* note 2 (describing peer-to-peer file sharing software as an effort to affect the regulatory environment for copyrighted works). For purposes here, however, the analysis considers the more typical policy lever of legal regulation.

<sup>76</sup> The description of property rules and liability rules as defining the basic forms of legal rules was established in Calabresi and Melamed’s seminal article, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, *supra* note 24.

Sections II and III, the choice of legal rule in this context has a traditional normative component (i.e., Which form of legal rule provides the best/most efficient regulatory mechanism?), and a distinctly instrumental component (i.e., Which form of legal rule most effectively influences the law-software equilibrium?). Analyzing the rule-forms in this light suggests that the real choice of legal rule in cyberlaw regulation is between (a) relatively strong property rules and (b) rules consisting of significant forms of legal preemption; absent the support of legal preemption, liability rules appear to be significantly less attractive. As between these choices, any generalizable conclusion is relatively tentative, recognizing the deeply contextual nature of any regulatory undertaking in cyberspace. There is at least some reason to believe, however, that in a broad array of cases, a property rule will outperform those based on stronger forms of legal preemption.

#### *A. Property Rules, Liability Rules, and Legal Preemption*

In any evaluation concerning forms of legal regulation, it is customary to discuss the issue in terms of two basic forms of legal rules: property rules and liability rules.<sup>77</sup> A property rule grants the rightsholder (the ‘property owner’) the right to enjoin unwanted uses, and thus forces bargaining between owners and users to determine the details of the use (such as price, terms of use, etc.).<sup>78</sup> For example, in the cyberproperty context, a property rule establishes the basic right of web developers to determine access—and presumes that contractual arrangements would define the details of such access. A liability rule, by contrast, defines much of the details of the arrangement—typically allowing use except where certain defined harms occur, whereupon a remedy (usually monetary) will be granted.<sup>79</sup> Again, in the cyberproperty context, a liability rule would grant access, subject to harmful acts that would trigger liability—for

---

<sup>77</sup> See, e.g., Abraham Bell & Gideon Parchomovsky, *Property Rules*, 101 *Mich. L. Rev.* 1, 3 (2002) (“The Calabresi-Melamedian typology has been widely understood to exhaust all possible ways of protecting legal entitlements, and the binary system they devised has dominated legal thought and scholarship.”). See also Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 *Cal. L. Rev.* 1293 (1996); Louis Kaplow & Steven Shavell, *Property Rules Versus Liability Rules: An Economic Analysis*, 109 *Harv. L. Rev.* 713 (1996); Symposium, *Property Rules, Liability Rules and Inalienability: A Twenty-Five Year Retrospective*, 106 *Yale L.J.* 2081 (1997).

<sup>78</sup> Calabresi & Melamed, *supra* note *supra* note 24 at 1092.

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

example, extreme overuse of bandwidth,<sup>80</sup> or forms of linking bordering on misappropriation.<sup>81</sup>

It is widely argued that, following Cosean reasoning, property rules are better suited for circumstances where cost-effective bargaining is possible—because they are more likely to result in welfare-enhancing arrangements than liability rules.<sup>82</sup> However, where transaction costs are high, or bargaining is not possible, liability rules are the better choice.<sup>83</sup>

Yet the binary choice of legal rule-form is fundamentally incomplete in the cyberlaw context.<sup>84</sup> This observation follows from the basic code-meets-law point noted above, and is the same reason that simply establishing a legal rule does not necessarily determine (and may not even predict) the regulatory condition that results—both law and software regulate in cyberspace, and both must be accounted for in the analytic approach.<sup>85</sup> Thus, the choice of legal form must contain an additional dimension, one that recognizes and reflects the crucial interactions between law and software.

One way this additional dimension takes form is by the inclusion of a third form of legal rule—described here as *legal preemption*, that directly addresses the regulatory effects of software.<sup>86</sup> Legal preemption, then, has as its goal the fixing (at least within a narrow range) of the equilibrium point on the law-software interface, and thus allowing—at least in theory—greater predictability and stability in the software component of the overall regulatory condition.

---

<sup>80</sup> Perhaps by knowingly triggering the “slashdot effect,” a spontaneous high hit rate upon a web server due to posting links to its content on a high-volume news site, named after the web site slashdot.org. See, e.g., Stephen Adler, *The Slashdot Effect: An Analysis of Three Publications*, at <http://ssadler.phy.bnl.gov/adler/SDE/SlashDotEffect.html>. The Slashdot effect has been known to cause web servers to become unreachable or to crash altogether.

<sup>81</sup> For example, inline linking of others image, see *Kelly v ArribaSoft*, or the framing of content (displaying content from another site in a ‘frame’ in a web page such that it appears to be a part from the local site).

<sup>82</sup> Calabresi & Melamed, *supra* note 24, at 1108-10.

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

<sup>84</sup> Bell and Parchomovsky have posited that the analysis is incomplete in other contexts as well, and that a variety of ‘mixed’ or ‘dynamic’ versions of property rules and liability rules exist—which they describe as ‘pliability rules.’ See Bell & Parchomovsky, *supra* note 77, at 4. To some degree, the hybrid forms of traditional legal rule-forms and legal preemption described here are related to their concept of pliability rules.

<sup>85</sup> See *supra* Section II.

<sup>86</sup> Lessig describes this phenomenon as “law regulating code”. Lessig, *Horse*, *supra* note 1, at 530-32.

There are several possible forms of this regulatory technique, ranging generally from strong forms to weaker versions. The strongest approach is what might be described as a *direct* form, where the legal code directly establishes formal boundaries or requirements for software code. For example, the Audio Home Recording Act defines the permissible workings of hardware-and-software “digital audio recording devices,” specifying that the software will implement a copyright management system, known as the Serial Copy Management System.<sup>87</sup> Other examples include the ongoing legislative and regulatory proposals requiring a “broadcast flag” to be included in the signal for digital television, so as to allow for the operation of copy management software.<sup>88</sup>

Another, somewhat less strong form is regulatory *standardization*, where legal regulations establish the framework within which software will operate. For example, the FCC has established (repeatedly) the technical standards for digital television (HDTV).<sup>89</sup> While not directly mandating the particulars of the software, establishing the standards will of course greatly reduce the variability of the technologies used.

A weaker-but-related version of equilibrium enforcement is legal regulation that *supports* software-as-regulator—the paradigmatic example here being the Digital Millennium Copyright Act (DMCA), which generally forbids the distribution of technologies that allow circumvention of DRM systems protecting copyrighted works.<sup>90</sup> In the analytic framework established by this paper, these supportive regulations serve to stabilize the law-software equilibrium point, by reducing the incidence of at least some forms of anti-regulatory code.<sup>91</sup> Note that, perhaps counter-intuitively (but relevantly to the analysis here), this form of regulation may serve to actually *reduce* the regulatory effects of software: once the level of software protection required to trigger the supportive law (for example, the DMCA describes this as “effective[]” protection)<sup>92</sup> is reached, there will be diminished incentives to seek stronger software effects, given that no additional legal protection will be

---

<sup>87</sup> See 17 U.S.C. § 1002(a) (2002).

<sup>88</sup> Amy Harmon, Hearings Set On Measure To Promote Digital TV, The New York Times, September 25, 2002, p. C7.

<sup>89</sup> Edmund L. Andrews And Joel Brinkley, The Fight for Digital TV's Future, The New York Times, January 22, 1995, p. C1.

<sup>90</sup> See 17 U.S.C. § 1201 (2002).

<sup>91</sup> See Wu, *supra* note 2, at 132-35 (describing the effects of anti-regulatory code in changing the regulatory condition for copyrighted goods).

<sup>92</sup> See 17 U.S.C. § 1201(a)(1) (2002)



achieved, and the incidence of anti-regulatory code will be reduced.

A fourth—and perhaps weakest—form of legal preemption would be legal rules that specify the use of particular software in a *transactional* rather than regulatory manner. For example, consider a legal requirement that transactions concerning privacy utilized the P3P standard,<sup>93</sup> or that web pages were to be tagged according to the PICS standard, to allow for content filtering and selection:<sup>94</sup> each has a comparatively small regulatory component, their chief aim being to establish a transactional framework.<sup>95</sup>

Table 1 summarizes the spectrum of legal preemption.

Strong Forms			Weak Forms
<i>Direct</i>	<i>Standardization</i>	<i>Support</i>	<i>Transactional</i>
AHRA	FCC activities	DMCA	P3P or PICS mandate

**Table 1: Forms of Legal Preemption Rules**

As should be apparent, the above categories are neither exhaustive nor mutually-exclusive. Indeed, many forms of legal preemption rules will involve a mixture of the above. As will be discussed more fully below, however, the form of the legal preemption rule has important implications for the analysis.

The broader point, however, is this: just as the choice of a legal rule will involve analytic trade-offs between the familiar categories of property rules and

---

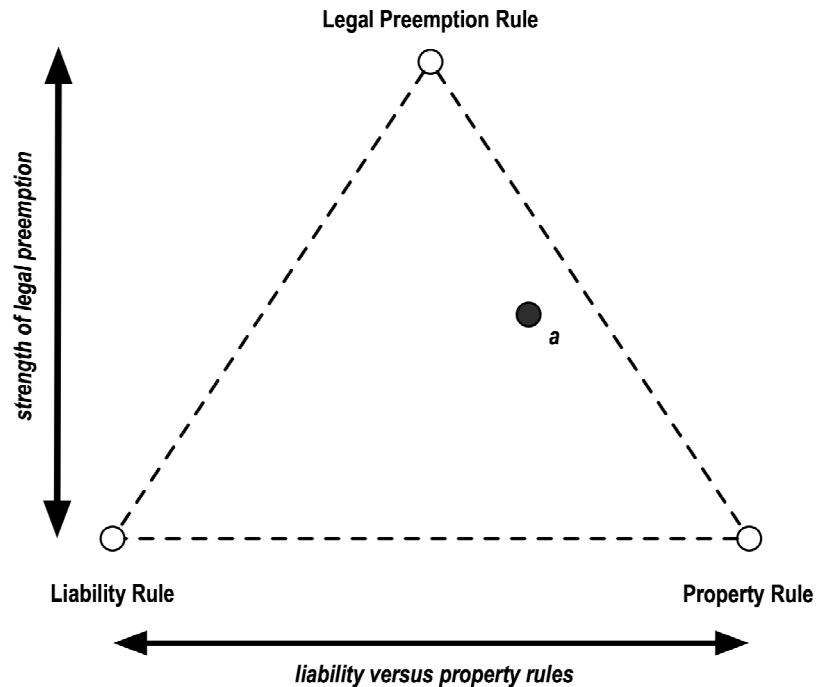
<sup>93</sup> P3P is the acronym for the Platform for Privacy Preferences, a technical standard developed to enhance the ability of users to determine the use of their personal information online. See World-Wide-Web Consortium, Platform for Privacy Preferences (P3P) Project, at <http://www.w3.org/P3P/>.

<sup>94</sup> PICS stands for the Platform for Internet Content Selection, a technical standard for associating labels with web content. One promising use of PICS is as a means for filtering web content for children and minors, though the standard is not so limited. See World-Wide-Web Consortium, Platform for Internet Content Selection (PICS), at <http://www.w3.org/PICS/>. For a detailed discussion of the possibilities and challenges (including constitutional) of forms of a mandatory PICS scheme, see generally R. Polk Wagner, *Filters & the First Amendment*, 83 Minn. L. Rev. 755 (1999).

<sup>95</sup> Of course, as any lawyer will note, even transaction/procedural rules have substantive effects; thus transactional forms of legal preemption rules will clearly have some regulatory effects. The point here is to try to tease out some general distinctions for more fine-grained policy analysis.

liability rules, the incorporation of legal preemption rules in the cyberspace context will require a similar exercise along an additional dimension—the impact that the legal rule will have on corresponding software regulation (and thus the effect on the law-software interface).

Figure 3 depicts this multidimensional analysis.



*Figure 3: The Dimensions of the Choice of Legal Rule*

Point *a* in Figure 4 represents a possible analytic location of a legal rule, containing a combination of features from liability rules, property rules, and legal preemption rules. Any choice of a legal rule in cyberspace will have this form of multidimensional analysis; both axes of regulatory choice will impact the quality and nature of the legal effect.

### *B. Choosing the Form I: Normative Analysis*

Having identified the dimensions along which the analysis must take place, the next step is to comparatively evaluate the benefits of a choice of legal rule-form. Here again there is an important complication in the cyberlaw context: because the policy lever of the legal rule must be understood (given Sections II

and III above) as operating both to establish a legal regulatory effect (i.e., protection or entitlement) and to generate a software-regulatory response, the choice-of-form analysis includes both normative and instrumental components.<sup>96</sup> The normative component is well understood: Which legal rule is likely to best provide the desired legal effects.<sup>97</sup> The instrumental component considers the legal rule in the context of its impact on software regulation, and asks which rule form is likely to be more effective at influencing the software response. Each of these evaluations must of course be conducted for each dimension of regulation (see Figure 3)—property versus liability rules, and strength of legal preemption.

### 1. Property versus liability rules

The first step is to re-evaluate property rules and liability rules from a perspective that reveals their relationship with software regulations. The intent here is not to restate the standard set of competing advantages and disadvantages of the property rule versus liability rule debate.<sup>98</sup> Instead, the analysis focuses on those factors which appear to take on heightened relevance in the cyberlaw context, and evaluates how these play out. Thus, to a degree, the analysis here is relative—noting changes in the analysis due to the special regulatory environment of cyberspace.

As noted above, regulatory environments featuring software content are generally characterized by dynamic changes in the regulatory environment (as a result of technological changes), and very complex interactions between the legal rules and software techniques.<sup>99</sup> This suggests that three factors in particular are especially relevant. First, the flexibility accorded to the parties involved, both to assist innovation in the dynamic environment, and, more importantly, to respond to changes in the regulatory condition. As was described in Section II above, the ability to dynamically respond to changing conditions is important to stability in the regulatory environment. More flexibility is likely to be far better in this context.

Second, the level of routine institutional intervention—the participation of the judiciary or regulatory agencies, for example—is important. In a rapidly-developing and complex regulatory environment, there are potentially-

---

<sup>96</sup> See *supra* notes 46-48 and accompanying text.

<sup>97</sup> See, e.g., Calabresi & Melamed, *supra* note 24, at 1105

<sup>98</sup> See, e.g., *id.* at 1101.

<sup>99</sup> See *supra* notes 44-48 and accompanying text.

significant costs in uncertainty and errors resulting from additional (and customary) institutional intervention.<sup>100</sup>

A third factor is the responsiveness of any legal rule. As was described above, changes in the software regulatory context can dramatically alter the overall regulatory condition.<sup>101</sup> Hence the ability to change the effects of a legal rule is important; more responsive legal rules are far more likely to be beneficial.

Two additional factors seem quite relevant to the analysis here, given the cyberlaw context. The first is transaction costs, which are of course a generic concern related to legal rules.<sup>102</sup> And yet the great scale of the online environment suggests that transaction costs deserve heightened attention here; any change in transaction costs as a result of reliance on a property-type rule is likely to be significant, due to the huge multiplier effect of the number of transactions conducted (or potentially conducted) online.

The last (but not least) relevant factor is the question of embedding public values—such as free speech, diversity of opinion, privacy, etc.—into the regulatory construct.<sup>103</sup> Like transaction costs, this issue is typical of many choice of legal-rule analyses; the question here is whether it is especially relevant in the online world. Larry Lessig, among others, has forcefully argued in the affirmative: on the general grounds that the Internet (and related technologies) offers society a great opportunity to expand our social structures, to enhance diversity, expression, and individualism.<sup>104</sup> And while there is at least some doubt as to its heightened import in the cyberlaw context, this is a widely-held view, and thus should be included in the analytic process.<sup>105</sup> Here, a

---

<sup>100</sup> See supra notes 61 and accompanying text. See also McGowan, supra note 26, at 16.

<sup>101</sup> See supra notes 36-43 and accompanying text.

<sup>102</sup> See, e.g., Calabresi & Melamed, supra note 24, at 1103; Bell & Parchomovsky, supra note 77, at 4.

<sup>103</sup> See, e.g., Lessig, Horse, supra note 1.

<sup>104</sup> See, e.g., Lessig, Code, supra note 1, at 8. See also Elkin-Koren, supra note 26; O'Rourke, Shaping Competition, supra note 26, at 1978.

<sup>105</sup> The counterarguments take one of two forms. The first is to question the premise of Internet exceptionalism that underlies many arguments related to the great public import of the Internet. Surely the 'net is very important, the argument goes; but then again so are a huge variety of realspace regulatory environments—many of which might arguably be said to have a more direct impact on most people's lives (i.e., equality, social entitlements). See, e.g., Easterbrook, supra note 8; Goldsmith, supra note 8.

The second response generally accepts the Internet exceptionalism premise, and yet suggests that the best way to ensure that its potential is maximized is to largely leave the decisions in the hands of private individuals. That is, this response emphasizes that much (if

liability rule, by allowing more control over the arrangements, will allow more public values to be reflected in the regulatory environment.

Table 2 maps these factors onto the features of property and liability rules, describing in relative terms the rules' performance related to each factor.

<b>Rule Form</b>	<b>Flexibility</b>	<b>Institutional Intervention</b>	<b>Response Time</b>	<b>Transaction Costs</b>	<b>Embedding Public Values</b>
Property Rule	High	Low	High	High	Low
Liability Rule	Low	High	Low	Low	High

*Table 2: Features of Property versus Liability Rules*

Whether one is convinced that the results displayed in Table 2 point strongly (or at all) in the direction of a particular form of legal rules will depend largely upon a (normative) judgment about the relative importance of each factor. In this sense, of course, the analytic process is much like a more traditional choice of legal rule-form.<sup>106</sup> Yet the value of setting forth the process goes beyond that, for two reasons. First, recall that such analytic approaches are deeply contextual; thus in any particular application (i.e., regulatory issue), certain factors may be deemed more important than others. For example, the argument in Section V below posits that in the cyberproperty context, allowing great flexibility in setting access conditions is particularly important to continued innovation on the World Wide Web; thus a property rule might be said to be at least weakly favored by this analysis.<sup>107</sup>

The second important insight is that simply understanding the respective strengths and weaknesses can suggest to policymakers ways of combining, for example, property rules and legal preemption. For example, the results in Table 2 suggest the value of considering a hybrid property rule and a legal preemption rule directed to enabling transactions—thereby reducing a disadvantage of the property rule-form.

---

not most) of the explosion related to the 'net is the result of private decision-making (sometimes, but not always motivated by profit), and that absent serious indicators otherwise, government interference should be minimized. See, e.g., R. Polk Wagner, Information Wants to be Free, 103 Colum. L. Rev. 995 (2003).

<sup>106</sup> See, e.g., Calabresi & Melamed, *supra* note 24, at 1103.

<sup>107</sup> See *infra* notes 147-157 and accompanying text.

## 2. Strength of legal preemption

As noted above, a rule of legal preemption has as its goal the fixing (or influencing, in weaker form) the corresponding regulatory effects of software.<sup>108</sup> Therefore, the series of concerns raised about the use of software as a regulatory mechanism do suggest that legal preemption rules offer at least potentially-attractive options. Indeed, this is the chief advantage of a legal preemption rule, and it is likely to be significant. This enthusiasm, however, should be tempered by a recognition of limitations that seem inherent in any such regulatory approach. The analysis that follows suggests three considerations: the difficulty in directly addressing software in legal regulations; the increased cost of error inherent in any legal preemption scheme; and concerns about institutional competence.

Consistent with the points made in Section II above, software development is a rapidly moving, nearly unpredictable target—making legal regulations that directly address software difficult indeed.<sup>109</sup> Not impossible, certainly, but quite difficult as a technical matter; as noted above, the precise details of the law-software interface are deeply complex, and attempting to codify those in any meaningful way is clearly a nontrivial exercise.

Following from the difficulty point, note that the costs of error in engaging in direct regulation of software effects could be far more significant than the error involved in setting legal regulation alone. For example, a too-low level of legal protection in the cyberspace context may be partially overcome by the effects of software regulation. However, the combination of both too little law and direct software regulation (of the preemption form, perhaps) would be far more problematic. To take another example, serious problems could arise if the legal regulation encompassed more forms of software than intended, thus resulting in potentially-serious unintended consequences. Indeed, this is an oft-heard criticism of the DMCA—that its scope is such as to encompass business practices<sup>110</sup> and even bona fide research<sup>111</sup> well afield from the support of basic

---

<sup>108</sup> See supra notes 77-95 and accompanying text.

<sup>109</sup> See supra notes 50-65 and accompanying text.

<sup>110</sup> See, e.g., Dan L. Burk, *Anti-Circumvention Misuse*, 50 *UCLA L.REV.* 1095, 1110-14 (2003).

<sup>111</sup> See, e.g., David P. Hamilton, *Professor Savors Being in Thick of Internet Rows*, *WALL ST. J.*, June 14, 2001, at B1; Jennifer 8. Lee, *In Digital Copyright Case, Programmer Can Go Home*, *N.Y. TIMES*, Dec. 14, 2001, at C4; Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 *Yale L.J.* 1575, 1646-49

DRM systems. Errors when seeking to directly regulate the law-software interface could be quite serious.

Finally, though not entirely unrelatedly, the question of direct regulation of software raises questions of institutional competence. As was noted above, there are reasons to think that judges in particular are not well-suited to engage in meaningful software-regulatory-policy analyses. Legislatures or regulatory bodies might have a better chance, but the rapid developing environment suggests that any move to take the path and pace of software development away from private decision-makers is one that must be viewed skeptically. There are likely to be conditions where this approach nonetheless makes sense, but the point here is that great care must be taken in this direction.

Note of course that, as noted above, the various forms of legal preemption rules raise differential concerns—as a general matter, the less strong, less interventionist forms of legal preemption are less likely to have the problematic side-effects. In any event, it does seem clear that despite the limitations, legal preemption rules would be consistent, at least in some circumstances, with the analytic framework developed here. Their suitability in any particular case, of course, is dependent on a variety of contextual factors, as well as the balance of the normative and instrumental analysis.

### *C. Choosing the Form II: Instrumental Analysis*

The instrumental analysis of the choice of legal rule-forms is primarily concerned with the *effectiveness* of the rule in influencing the location of the law-software equilibrium. That is, legal rules in the cyberspace context serve both to establish legal effects and to influence the corresponding software-regulatory effects. Indeed, as Section III demonstrated, there is good reason to believe that in many cases, a major goal of the legal regulation will be to affect software regulation—usually by reducing it. The following section steps through the analysis of the instrumental effects of the choice of legal rule.

#### 1. Property versus liability rules

As noted in Section II above, absent direct regulatory effects (legal preemption), the law-software equilibrium for a particular regulatory condition

is generally determined by private decision-making related to the cost-benefits of each regulatory effect (law and software). Thus, to influence the law-software equilibrium, a (non-preemptive) legal rule must provide an attractive alternative to regulation-by-software.

As between a property rule and a liability rule, there are at least two reasons to believe that the property rule will more effectively influence the law-software equilibrium. The first is the potential strength of the legal effects: a reasonably-broad property rule will allow rightsholders the ability to set restrictive conditions for access—even quite stringent ones—without the need to resort to software regulation. A liability rule, by definition, is more conditional in nature; it will have less potential legal effects, and thus a weaker influence on the quantum of software effects. Put more directly, because a liability rule offers less potential protection (legal effects) to rightsholders, it is less likely to discourage the use of software regulations.

The second important reason a property rule is likely to more significantly influence the law-software equilibrium is its flexibility. By allowing rightsholders to structure access in virtually infinite ways, a property rule is likely to provide important benefits over regulation-by-software—which, as noted in Section III above, is, as a general matter, relatively inflexible.<sup>112</sup>

Here, both the potential strength of the legal effects and the flexibility in arranging rights suggest rather strongly that a property rule clearly dominates the liability rule in an instrumental analysis. Indeed, the key feature of the liability rule—fixed legal effects—would seem to call into serious question the rule’s ability to have significant instrumental effects at all. By fixing legal effects, a liability rule will almost definitionally be an unattractive alternative to software regulation, which offers at least some flexibility—albeit far less than a property-type legal rule. So it may be that in instrumental terms, a liability rule, standing alone, is virtually no option at all. (Note, of course, that a liability rule coupled with legal preemption will certainly have significant effects on the law-software equilibrium.)

## 2. Strength of legal preemption

In considering the instrumental effect of legal rules—the effectiveness of the influence a legal rule is likely to have over the law-software equilibrium—the advantage is manifest: a rule including legal preemption will (by definition) have

---

<sup>112</sup> See, e.g., Epstein, *supra* note 26, at 84 (noting the particularization and standardization achievable in contractual agreements); McGowan, *supra* note 26 at 30.



significant effects on the law-software interface. Depending upon the level of intervention, these effects can range from almost complete determination of software regulations to indirect encouragement.

There are, of course, at least potentially-significant downsides. First, and most obviously, legal preemption requires a trade-off between the advantages inherent in software regulation—especially flexibility—and the effectiveness of the rule in fixing the law-software interface. That is, strong forms of legal preemption (banning certain technologies, for example) will have great effects, but they will also remove an important component of regulatory flexibility from the system altogether. Weaker forms of legal preemption, of course, will not remove all such flexibility—but they will also have more attenuated effects.

A second important concern, though related to the first, is that the use of legal preemption increases the costs of error inherent in regulatory decision-making. That is, assume for the moment two legal rules in the cyberspace environment, each establishing the same legal effects X (i.e., the same amount of legal protection): the first is a traditional legal rule (i.e., one without preemption); the second is a rule including strong legal preemption aspects. If the quantum of legal effects X is somehow inappropriate or in error—perhaps the protection is too weak to support the development desired, or is over-strong, given public policy considerations—then we can expect the regulatory environment in the first case to adapt to at least some degree, by using additional software regulation to complement the legal regulation. The result will be that the cost of error is likely to be reduced, at least somewhat. But in the second case, the legal preemption will restrict or eliminate this adjustment, so the error is likely to be more costly. In other words, introducing legal preemption in effect ‘raises the stakes’ of the policy judgment, and thus increases the chances for costly (or even enormously costly) errors.

#### *D. Choosing the Legal Rule in Cyberspace*

This section has outlined the implications of incorporating a more meaningful understanding of the regulatory effects of software into the choice of a legal rule for cyberspace regulation. Such effects can be (and, indeed, must be) accounted for, but the analytic process is unquestionably more complicated. In particular, the foregoing suggests that the traditional dichotomy between property and liability rules must be expanded to include rule forms that directly effect the quantity and nature of software regulation—legal preemption. This implies that the choice of rule-form occurs in two dimensions: a choice not only between property rules and liability rules, but also between legal preemption rules and more pure legal forms.

Another key finding here is that the decision-making criteria must also be expanded to incorporate the instrumental effect of legal rules—the effectiveness with which the rule influences the law-software equilibrium. Indeed, if one agrees with the analysis in Section II above, that in many cases software regulation is a poor substitute for legal regulation, this instrumental performance may be as important as the more traditional normative analysis of the ‘goodness’ of a legal rule-form.

Although the choice of legal rule-form here is revealed to be deeply complex and contextually dependent upon legal and technological circumstances, there are a few general observations that spring forth. The first is that what might be called ‘naked’ liability rules—those without aspects of legal preemption—appear to be markedly less suitable for cyberspace regulation than either ‘naked’ property rules, or liability rules with some significant support from legal preemption rules. This might suggest that: (1) the real choice of rule-forms in the cyberspace context is between property rules and hybrid liability-legal preemption rules; and (2) that legal preemption rules are particularly interesting as policy options. The second general observation is the ability to mix forms of traditional legal rules (property rules, liability rules) with forms of legal preemption rules. In particular, consider the ability to use a property rule combined with, for example, a transactional form of a legal preemption rule—thereby addressing the concern about transaction costs that attached to property rules. In addition, such hybrid rules suggest that careful policy analysis can tailor legal-rule forms to address quite closely the particulars of a given regulatory context in cyberspace.

## V

## THE CASE OF CYBERPROPERTY

This Section follows from the prior three, by applying the foregoing analysis to one of the more controversial regulatory issues in this area: *cyberproperty*. As used here, a “cyberproperty” right is generally a right to exclude others from access to network-connected resources.<sup>113</sup> That is, a cyberproperty right will allow owners to determine the details of the use of, for example, their web sites, email systems, and the like. Paradigmatically, the cyberproperty right would include a right to deny http ‘links’ to the web site from another’s web page.

So defined, the cyberproperty right analyzed in this section is intended to conceptually encompass a range of emerging and related legal actions, each with different doctrinal foundations.<sup>114</sup> This range of doctrinal approaches, along with a few of their important features and regulatory effects, are described briefly below. However, the goal of this Section is not to engage in the sort of detailed doctrinal analysis that has been an important part of earlier contributions, nor even to suggest doctrinal ‘fixes’ to better establish the cyberproperty right. Instead, the purpose here is to use the regulatory confusion surrounding this important question as a hook upon which to hang a broader form of policy analysis, following the lessons of the Sections above.

---

<sup>113</sup> I recognize that the invocation of the term ‘property’ here suggests an analogical connection between access protections online and those in realspace—i.e., real ‘property’. As should become clear below, however, this analysis does not place weight on real property premises.

<sup>114</sup> Table \_ below notes the variety of (legal) sources from which the cyberproperty entitlement might be said to emanate. Taken collectively, these recent legal developments represent a penumbra of rights surrounding the issue of access to network-connected resources; the term cyberproperty is used both as a shorthand for these developments, as well as a means by which the detailed doctrinal controversies can be laid aside in favor of broader analytic work.

There exist several important works considering the general issue of cyberproperty. See, e.g., Richard Epstein, *Cybertrespass*, 70 U. Chi. L. Rev. 73 (2003); David McGowan, *Website Access: The Case for Consent*, \_\_ Loy-Chi. L. J. \_\_ (forthcoming 2003); Trotter Hardy, *The Ancient Doctrine of Trespass to Websites*, 1996 J. Online L. art. 7; Dan L. Burk, *The Trouble With Trespass*, 4 J. Small & Emerging Bus. Law 27 (2000); Nina Elkin-Koren, *Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing*, 49 J. copyright Soc’y 165 (2001); Maureen O’Rourke, *Property Rights and Competition on the Internet: In Search of An Appropriate Analogy*, 16 Berkeley Tech. L. J. 561 (2001); Maureen O’Rourke, *Shaping Competition on the Internet; Who Owns Product and Pricing Information?*, 53 Van. L. Rev. 1965 (2000).

It is clear that, whatever the current state of cyberproperty, rights of access in cyberspace is a hotly-contested issue. The trespass to chattels approach to this issue in particular has been hotly contested among legal scholars recently—especially doctrinally<sup>115</sup>—though similar concerns have been noted with respect to the other approaches as well. Normatively, the emergence of cyberproperty has led scholars to declare the imminent demise (in early 2000) of search engines,<sup>116</sup> as well as to describe the current state of affairs as “nothing short of disastrous for public policy.”<sup>117</sup> Others take a more sanguine view, arguing that the intellectual tradition (and widespread success) of real property entitlements suggest that these developments are likely to be socially beneficial, in part by facilitating the bargaining (and thus diversity of arrangements) that is essential to continued growth of the Internet.<sup>118</sup>

The analysis in this section begins by noting that the regulatory environment—both law and software—for the cyberproperty right is complex, uncertain, and unstable, suggesting that policy changes are necessary and appropriate. The analysis then considers the appropriate content of the law-software interface, by mapping the key policy imperatives onto the present technological realities. These factors include:

- (a) the fact that the vast majority of online resources are offered in a “full access” condition, and that therefore a relatively small number of owners should be expected to opt for the more nuanced “conditional access” modes that a cyberproperty right allows;
- (b) the need for flexibility in structuring online information delivery and business models;
- (c) a recognition of the important public good aspects of open access to network resources; and
- (d) the benefits of establishing a clear and stable regulatory regime;

In each case, the analysis suggests that the regulatory condition for cyberproperty should contain more law and less software. Furthermore, the choice of legal rule is also informed by this framework; a detailed understanding

---

<sup>115</sup> See, e.g., Dan Burk, *supra* note 26; O’Rourke, *Analogy*, *supra* note 26.

<sup>116</sup> See Brief of Amici Curiae in Support of Bidder's Edge, Inc. at 2- 3, *eBay v. Bidder's Edge, Inc.*, 100 F. Supp. 1058 (N.D. Cal. 2000) (No. 00- 15995), *available at* [http://jurist.law.pitt.edu/amicus/biddersedge\\_v\\_ebay.pdf](http://jurist.law.pitt.edu/amicus/biddersedge_v_ebay.pdf) (last visited Mar. 9, 2004).

<sup>117</sup> Lemley, *Place and Cyberspace*, 91 Cal. L. Rev. 521, 523 (2003).

<sup>118</sup> See, e.g., McGowan, *supra* note 26; Epstein, *supra* note 26.

of the relationship between law and software argues, with at least some force, in the direction of a property rule rather than a liability rule, and there is some support for the imposition of legal preemption rules as well. Indeed, an interesting result that emerges from the analysis is the possibility of a hybrid form of rule: one that combines a fairly strong property rule, with a default condition in favor of open access, and encourages software techniques to implement transactional forms.

Note that for simplicity, the analytic discussion that follows will be considering the cyberproperty right in terms of its specific application to the World Wide Web—that is, access to web sites / servers. Similar analyses would be followed for related applications involving other network-connected resources, such as email systems, for example.

#### *A. The Legal-Software Landscape of Cyberproperty*

Consistent with the analytic framework developed in Section II this article, this part notes the present state of regulatory conditions—both law and software—in the cyberproperty context. As noted above, the cyberproperty right is at least partially supported by several legal doctrines, ranging from trespass law to the Computer Fraud and Abuse Act (CFAA).<sup>119</sup> Table 3 outlines the basic features of these doctrinal hooks, and considers the scope of their legal effects.

<b>Doctrine</b>	<b>Protection</b>	<b>Key Case</b>	<b>Regulatory Effects</b>
Trespass to Chattels	Unauthorized access to physical servers	eBay v. Bidder's Edge <sup>120</sup>	Medium: Relatively strong, though doctrinal uncertainty concerning damages.
Copyright Law	May protect certain forms of 'inline' linking	Kelly v Arriba Soft <sup>121</sup>	Unclear: serious questions of applicability to this context; fair use defenses exist
(Naked) Contract Law	Implements 'Terms of Service Agreements' posted on page	Register.com v Verio <sup>122</sup>	Medium: limited to web pages, etc.; some uncertainty about consent

<sup>119</sup> 18 U.S.C. § 1030 (2002).

<sup>120</sup> eBay, Inc. v Bidder's Edge, Inc., 100 F.Supp.2d 1058 (ND Cal. 2000).

<sup>121</sup> Kelly v Arriba Soft Corp., 280 F.3d 934 (9<sup>th</sup> Cir. 2002), opinion withdrawn by Kelly v. Arriba Soft Corp., 2003 U.S. App. LEXIS 13557 (9<sup>th</sup> Cir. Cal., July 7, 2003).

<sup>122</sup> Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (SDNY 2000).

CFAA	Unauthorized intrusion into computer systems.	Register.com v Verio <sup>123</sup>	Medium: Potentially strong, though intended to prevent hacking; mental state requirement
------	---	-------------------------------------	--

**Table 3: The Legal Environment for Cyberproperty**

As Table 3 demonstrates, a legal infrastructure of the cyberproperty right exists, but its net effects are far from clear. In particular, note the relatively high degree of uncertainty about the scope of the regulatory effects; as applied to this issue, each doctrinal approach includes significant conceptual analytic difficulties, which tend to both reduce the net regulatory effects, as well as increase the instability and uncertainty of the legal framework.

Table 3, then, by demonstrating the deeply unclear nature of the cyberproperty entitlement, provides a hook by which to begin the policy analysis.

Next, Table 4 sets forth the software-regulatory framework. (Note that this table looks specifically at access to web servers; the options for controlling access to other network resources are even more limited.)

Technology	Complexity	Effectiveness	Flexibility	Regulatory Effects
http_referer (server-side) <sup>124</sup>	High: requires CGI development/ software installation & configuration on server	Low: obscuring referrer header avoids it	Low: considers only referring page	Low: Depends upon default implementation
http_referer (Javascript)	Low: simple one-line code in html document	Low: obscuring referrer header avoids it	Low: considers only referring page	Low: Depends upon default implementation
Cookie redirection <sup>125</sup>	Medium: requires either CGI scripting or complex javascript	Low: cookie rejection is typical	Medium: cookies offer flexibility in information, but this generally requires prior visits	Medium

<sup>123</sup> Id.

<sup>124</sup> See, e.g., Exceptional Digital Enterprise Solutions, Inc., HotLinkStop, at <http://xde.net/xq/tool.hotlinkstop/qx/index.htm>; Simson Garfinkel, Web Security & Commerce 293-309 (1997).

<sup>125</sup> See, e.g., PerlscriptsJavascrpts.com, Redirection Cookie, at [http://www.perlscriptsjavascrpts.com/js/cookie\\_redirect.html](http://www.perlscriptsjavascrpts.com/js/cookie_redirect.html).

Robot Exclusion Standard <sup>126</sup>	Low: simple text file at root of server	Medium: unenforced/voluntary, works only for robots	Low: only 'bots, only deny/allow entire directories	Low
Authentication (password protection) <sup>127</sup>	Very High: requires both substantial code and user management	High: denies access to all except those authorized	Variable: individual users can be given differential access	Medium: very effective, but only appropriate in limited circumstances
URL obscuring <sup>128</sup>	High: requires database-based site/server software installations	Medium: prevents linking/bookmarking, but access unimpeded	Low: causes potentially-serious difficulties for users	Medium

**Table 4: The Software Environment for Cyberproperty**

As with Table 3, the information in Table 4 reveals a complex picture. There are a variety of software-regulatory options, with widely varying levels of complexity, effectiveness, and overall regulatory effects. It is of course important to note that Table 4 represents the best available information as of Summer 2003; as noted above, technology is constantly changing, and ongoing developments may change the parameters.

Looking closely at Table 4, two observations seem especially important to understanding the law-software interface here. The first is the relative inflexibility of the available software options. Note that the only options with better than 'low' scores of flexibility were also quite complex to implement. As will become more clear below, this inflexibility in the software regulatory environment has important implications for the analysis here.

Second, and similar to the legal infrastructure, there is a fairly high level of uncertainty in the net regulatory effects. This—together with the variability in the options—implies that instability in terms of regulatory effects will be a concern.

Taken together, Tables 3 and 4 offer an insight into the deep complexity of regulatory-policy analysis in the cyberspace context. Diverse sources of legal regulation, each with inherent uncertainty, combine with an array of potential software regulation possibilities, also with markedly different features. This recognition illustrates again the necessity of careful, nuanced forms of regulatory analysis in this context; looking at either the law or the software is not enough.

---

<sup>126</sup> See, e.g., The Web Robots Pages, at <http://www.robotstxt.org/wc/robots.html>.

<sup>127</sup> See, e.g., Garfinkel, *supra* note 124, at 280-292.

<sup>128</sup> See, e.g., ColdLink Bandwidth Protection Software, <http://coldlink.com/?qt=13>

And in fact, the complexity of the law-software interface is perhaps even greater than the brief overview above. For there is another layer that can be considered in this context—a look at particular applications of the cyberproperty right, and the differential ways that the two regulatory modes interact in a more detailed environment. For example, note that the question of http links to web pages can actually be subdivided into two applications: links to the ‘top’ pages of websites (i.e., links to *www.law.upenn.edu*) versus “deep linking” (i.e., links to *www.law.upenn.edu/fac/pwagner/research.html*). And while the legal infrastructure will operate in much the same way in each case, analyses of the software options change significantly. In particular, software regulatory techniques based on the `http_referer` header (which reports the referring web page) will become far more effective in the deep linking context. This is because, for web pages deep within the web site, the referrer-blocking mechanisms can be set to allow travel only from other internal pages, whereas the ‘top’ of the web site will by definition receive hits from a huge array of other pages (and blocking those is both more difficult and more prone to errors). This suggests that the software regulatory effects of this particular *application* of cyberproperty are likely to be greater than the general case outlined above—though the weaknesses noted above will of course be equally applicable. Again, this points out the complexities inherent in cyberspace regulation.

#### *B. The Limited Impact of a Cyberproperty Rule, and the Importance of Defaults*

After surveying the regulatory landscape—both law and software—for cyberproperty, the analysis turns to considerations of the basic facts of the current practices in this area. To this end, it is important to recognize the following observations. First, as demonstrated above, there are at least some forms of legal effects in place. That is, the various doctrinal hooks noted above offer website owners at least some legal protection against unwanted access. Second, again as outlined above, there also exists a range of software regulatory options, which can also serve a protective function in at least some respects. Together, these two factors of course suggest that the basic regulatory framework noted in Section II above is fully applicable—and that a key question here is to consider the equilibrium point. More important, however, is the recognition that, notwithstanding the existence of a legal-software regulatory condition, it appears that in the overwhelming majority of cases, owners of network resources are choosing to allow generally unimpeded access (referred to here as a “full access” condition). Precise numbers are virtually impossible to ascertain, but a reasonable estimate is that approximately 85 percent of web sites (for example) allow full access. A survey of the top 25 web properties found



that only one—*Ticketmaster.com*—appeared to restrict web linking, for example, in any way, whether legal or technological.<sup>129</sup> Of these, only about half used the robots exclusion standard (*robots.txt*) to restrict the use of web robots at all—and none excluded them entirely.<sup>130</sup> On the other hand, there are unquestionably a large number of web sites that are not publicly accessible—that use various technological means (passwords, access-restricting firewalls, etc.) to prevent access to virtually all resources (referred to here as a “no access” condition). Assume, for purposes here, that this group comprises about five percent of all web sites. Taken together, these estimates suggest that about 90 percent of web sites / web site owners want to allow either virtually full access to their sites, or want to severely limit access—or that only about ten percent want a more nuanced set of options (referred to here as “conditional access”).

One way to view this estimate is as an indictment of the entire exercise of cyberproperty. Arguably, in either the ‘full access’ or ‘no access’ cases, a cyberproperty regulatory condition is unnecessary: for ‘full access’, no regulation of any form is needed; and for ‘no access’ the technology exists (see “Authentication” in Table 2 above) to very effectively cordon off these sites. Thus the argument goes, why impose the costs and complexity of a regulatory environment when perhaps 90 percent of the interested parties are being reasonably well-served without it?

The problem with this approach is that it does not offer a meaningful solution to the remaining ten percent—who by definition desire to structure their activities in a way that lies between the ‘full access’ and ‘no access’ conditions: ‘conditional access’. For example, a web site owner might want to implement a business model that requires site visitors to traverse certain web pages, or to view certain advertising, or simply to ensure that users consider the offered materials in their intended context. Other developers may wish to restrict the types of uses that may occur within the web site, perhaps by enforcing rules for who can access and when. In each of these cases, neither the ‘full access’ nor ‘no access’ condition addresses the problem effectively.

---

<sup>129</sup> Top 25 according to June 2003 Nielsen/Netratings Data. See [http://www.nielsen-netratings.com/news.jsp?section=dat\\_gi](http://www.nielsen-netratings.com/news.jsp?section=dat_gi). *Ticketmaster.com* used a Terms of Service Agreement to forbid unauthorized deep-linking (but not linking to the top page). See <http://www.ticketmaster.com/h/terms.html>. It did not appear that any software regulation was used.

<sup>130</sup> The Robots Exclusion Standard is a voluntary standard to control the behavior automated web robots (also, ‘bots’ or ‘crawlers’), which are most typically used to index content for search engines. A web site owner can place a simple text file (names ‘*robots.txt*’) at the top level of the site; the file defines the scope of access for robots. See <http://www.robotstxt.org/wc/robots.html>.

There is no good reason to believe that the regulatory condition for cyberproperty should offer only the ‘full access’ or ‘no access’ choices. Indeed, there are very good reasons to believe that the class of individuals—albeit small, at an assumed ten percent—who desire more nuanced or detailed regulatory regimes, should be afforded an appropriate set of regulatory protections. One reason is that it is this ten percent that is most likely to represent innovation in business models (or models of presenting information) online. In an era where most such business models have been financial failures, continued innovation along this front is imperative to the long-term growth of cyberspace. Stated another way, to deny regulatory protections that would support innovation in web-based business models is to assume that we can somehow know and understand the ‘appropriate’ range of such models well into the future. And yet if there is one thing we do know about the future of cyberspace, it is that we likely haven’t even imagined it yet.

Another reason to believe that the regulatory condition for cyberproperty should address this ten percent is that doing otherwise would spur these web developers and entrepreneurs to take steps to alter the regulatory conditions themselves. For example, they might litigate over claims that to many appear weak.<sup>131</sup> This agitation is unlikely to be socially beneficial. For one thing, such efforts may succeed in ways that create unintended consequences; a judicial ruling may deeply change the underlying assumptions of the online world (say by flatly banning web links, or the like). But even if they don’t succeed, their agitation will almost certainly increase the uncertainty and instability across the board.

A third important reason that cyberproperty should encompass more complex options (than the binary “full access” or “no access” options noted above) is that, as David McGowan has explained, such protections are more likely to support an ecosystem of diverse online spaces.<sup>132</sup> Requiring web sites, for example, to allow all access or no access (or all-uses, as McGowan describes it) is more likely to be a recipe for homogeneity than a flourishing of differentiated sites.<sup>133</sup>

In sum, that the analysis of the cyberproperty right turns centrally on the needs of a relatively small group—on the (assumed) ten percent of network resource owners who desire the ability to set access rights in greater detail—does not present a substantial argument against such regulatory

---

<sup>131</sup> For example, this is a good explanation of *Kelly v ArribaSoft*, where Kelly was dissatisfied with the state of protection for his business model in selling his photos through his web site.

<sup>132</sup> McGowan, *supra* note 26, at 13-17

<sup>133</sup> *Id.*

conditions. What it does do, however, is point out important considerations for analysis when evaluating the appropriate balance between law and software.

The first such factor is the importance of establishing a clear default rule. Here, the recognition that the vast majority of network resources are offered without much access restrictions suggests: (1) that there are clear benefits to open access rules; and (2) that the costs of maintaining any cyberproperty regime will be far lower where the default condition is well-aligned with the prevailing activity. These observations argue in favor of both establishing a default rule and setting a relatively stringent requirement for overcoming the ‘full access’ default. By being quite clear about the rule, and by specifying a relatively high standard to change the default, any concerns about the ‘chilling effects’ of a cyberproperty regime would be eliminated.<sup>134</sup> Indeed, irrespective of the ultimate quantum of protection in the cyberproperty regime, this would clearly be an advantage over the present set of circumstances, where several doctrines offer possible legal remedies, and the question of notice is unclear.

Understanding the importance of the default rule influences the choice between law and software in this context. On balance, it suggests a move towards legal regulation rather than software, as the establishment of a default rule implies that those wishing to alter the rule will have to make at least some showing about the sufficiency of notice. This requirement of some ‘proof’ of clear notice of alteration would also minimize uncertainty among those utilizing the full access rights for most resources. Note that there may well be a role for software in transacting around the default rule (rather than establishing it): one possibility might be to require those wishing to alter the default rule of full access to utilize software techniques to provide notice concerning the changes, so as to further reduce transaction costs.<sup>135</sup> For example, one might establish a default rule in favor of unfettered web linking, and require any deviations from this rule to be noted in an electronic tag in the code of the web page (likely in addition to more traditional human-readable notice).<sup>136</sup> So for the all-important default rule, the analysis suggests that legal code should establish the parameters, and should perhaps directly regulate (mandate) software code as part of the process for altering the default condition in favor of full access.

---

<sup>134</sup> Here, for example, a single line in a Terms of Service Agreement would not be sufficient; far more direct forms of notice would be required.

<sup>135</sup> Larry Lessig suggested this possibility to the author, following from experiences with machine-readable licensing in the Creative Commons project. See <http://www.creativecommons.com/>. Note that a legal requirement for electronic notice is a form of direct software regulation noted (with tentative approval) in Section IV above.

<sup>136</sup> Perhaps a “meta” tag could be developed for this purpose.

### *C. The Flexibility Imperative*

As suggested above, there is perhaps no more important consideration in the context of cyberspace than the necessity, as much as possible, to maintain (and improve) the environment for innovation, experimentation, and entrepreneurship. Indeed, this might be safely said to be the hallmark of the Internet, and the World-Wide-Web in particular; the benefits received thus far from the inherent mutability of the ‘net have been enormous, and any policy analysis in this context must remain cognizant of this fact.

The value of flexibility in this context argues rather strongly in favor of a law-software interface that is more law and less software. As Table 2 amply demonstrates, many of the currently-available software regulatory techniques suffer from substantial problems related to inflexibility, especially those that are likely to have greater regulatory effect. For example, the `http_referer`-based techniques allow conditional access only on the basis of the referring page—perhaps better than no information at all, but unlikely to offer the broad range of flexible conditions that might otherwise be desired. The mechanisms related to cookies offer the promise of greater flexibility, stemming from a cookie’s ability to store a range of information. However, cookies require users to have prior history with the site, and are quite commonly erased, blocked, or altered by even technologically unsophisticated web surfers. But the basic point here is that all of the software options pale in comparison to the flexibility of contractual arrangements backed by property rights. Indeed, even a rule based on ‘nuisance’ or other legal definitions of harm, as recommended by Dan Burk,<sup>137</sup> would likely be more flexible than software regulation alone (though much less flexible than property rules and contracts). In any event, legal code has a substantial advantage over software code in this context—at least given current technological circumstances.

### *D. The Public Good of Network Access*

There can be little question that access to network resources (whether it be web linking, or access to email servers, etc.) has important public good effects—by facilitating the rapid exchange of information and ideas, as well as by allowing the rapid innovation and development cycles that are a hallmark of

---

<sup>137</sup> Burk, *supra* note 26, at 53. See *infra* note 143, and accompanying text.

the online environment. One argument that has consistently been made against a cyberproperty right is that such a regulatory condition would, by reducing web linking (for example), diminish the public good effects of the network. It is very far from clear, however, that this is true: following from the fact (noted in Part B. above) that only a small proportion of all networked resources would vary from an open access approach (and this seems to be by far the most reasonable assumption), then these concerns should be substantially reduced from the outset. Indeed, one might actually expect that the provision of a cyberproperty regulatory regime would prompt the shift of some networked resources (i.e., web sites) from a “no access” position to one of “conditional access,” or prompt the development and deployment of additional resources—thereby, in either case, increasing the quantity of accessible resources, and supporting the public good of access. Indeed, there seems to be little a priori reason to believe that the recognition of a cyberproperty right would meaningfully diminish the quantity or quality of access to network resources.

Yet the recognition of the desirability of access to network resources—especially “full access”—does offer insights into the law-software interface problem. First, it again emphasizes the importance of the establishment of a powerful default rule in favor of accessibility. As noted in Part B. above, this criteria argues rather strongly for a predominantly legal solution, though perhaps with software-implemented transacting.

Second, and perhaps even more importantly, consideration of the public good effects points out the need for a clear and stable regulatory regime. As Table 2 above (as well as the discussion in Section III) demonstrates, in this context, given the current state of technology, a predominantly legal framework seems far more likely to provide stability and clarity going forward.<sup>138</sup>

Third, as was noted in Section III above, software regulation is likely to be a relatively poor protector of the public interest inherent in regulatory conditions. Because software regulation does not require third-party intervention or consideration of enforcement costs, the expectation is that predominantly software-based regulation will be potentially more extreme and less stable than more traditional legal regulations.

Thus, the recognition of the public good aspects of access to network resources also argues (and rather strongly so) in favor of more law and less software in the regulatory condition.

---

<sup>138</sup> This argument assumes substantial clarification in the doctrinal framework for the cyberproperty right.

### *E. Clarity, Stability and Certainty*

A general goal of virtually any regulatory condition, but especially one in an emerging area of social and economic activity, is to establish relatively clear and stable rules of the game. As noted in Section III above, depending upon the particular circumstances of the technology, the desire for clarity and stability is likely to favor one regulatory mechanism—law or software—over another. In many cases, stability in particular is best served by legal regulation, as the rapid development of software regulatory technologies means that equilibrium conditions with large components of software regulation will be faster-changing (and thus more destabilizing).

### *F. Choosing Among Forms of Legal Regulation*

For each of the above issues, an analysis of legal versus software regulation suggests that the law-software equilibrium in the cyberproperty context should contain more law and less software. However, as noted in Section III above, there are a variety of forms of legal-regulatory approaches available; an important element in any policy analysis is evaluating these as well.

As noted above, the choice of legal rule in the cyberspace context contains two axes of inquiry.<sup>139</sup> The first is the fairly traditional dichotomy between property rules and liability rules—with the general argument being that property rules are better where the costs of bargaining are relatively low.<sup>140</sup> In the cyberproperty context, a property rule will establish the basic right of web developers to determine access—and presume that contractual arrangements would define the details of such access.<sup>141</sup> A liability rule, by contrast, defines much of the details of the arrangement—typically allowing use except where certain defined harms occur, whereupon a remedy (usually monetary) will be granted. In the cyberproperty context, a liability rule would grant access, subject to harmful acts that would trigger liability—for example, extreme overuse of bandwidth,<sup>142</sup> or forms of linking bordering on misappropriation.<sup>143</sup>

---

<sup>139</sup> See supra Section III.

<sup>140</sup> See supra notes 78-85 and accompanying text.

<sup>141</sup> See, e.g., McGowan, supra note 26, at 22.

<sup>142</sup> Perhaps knowingly triggering the ‘slashdot effect.’ See, e.g., Adler, supra note 80.

<sup>143</sup> For example, inline linking of others’ images, see *Kelly v ArribaSoft*, or the framing of content (displaying content from another site in a ‘frame’ in a web page such that it

The second dimension of analysis, however, is perhaps even more important: considering the utility of legal rules that involve forms of legal preemption—the direct legal regulation of software effects. In the cyberproperty context, legal preemption rules could range from the outright banning of certain software regulatory techniques (barring the use of cookies for access redirection, for example) by supporting software regulations (generally forbidding the obscuring of the `http_referer` header, for example), or by supporting transactional mechanisms (requiring the use of software to provide notice or enable transactions).

### 1. The False Choice: Property Rules versus Liability Rules

There have been important recent contributions to the debate concerning the choice between property and liability rules. Professors McGowan and Epstein, for example, suggest that bargaining is possible in this context, and that the property rule dominates.<sup>144</sup> Professors Burk and O'Rourke, on the other hand, contend that the sheer scale of the web access problem, as well as the important public values inherent in the (freely-networked) Internet, argue instead for a liability rule.<sup>145</sup> A recent decision by the Supreme Court of California comes down rather strongly in favor of liability rules (if any entitlement is indeed available at all).<sup>146</sup>

And yet, as the analytic framework of this Article has suggested, these now-familiar arguments on both sides of the property versus liability rule line lack the richness and contextual detail that is provided by incorporating aspects of software regulation into the analysis. For it is not quite as simple as property rules versus liability rules; the recognition of the participation of software regulation demands a more nuanced approach.

Table 2 from Section III above outlined the general framework for evaluation here, and it is worth revisiting that table here.

---

appears to be a part from the local site).

Dan Burk has suggested that a liability rule based on nuisance is the best option here, noting that such a rule would allow uses unless the costs of any access became “unreasonably costly.” Burk, *supra* note 26, at 53.

<sup>144</sup> See Epstein, *supra* note 26, at 84; McGowan, *supra* note 26, at 30.

<sup>145</sup> See Burk, *supra* note 26; O'Rourke, *supra* note \_\_\_.

<sup>146</sup> See, Intel v Hamidi, p. 25-28.

Rule Form	Flexibility	Institutional Intervention	Response Time	Transaction Costs	Embedding Public Values
Property Rule	High	Low	High	High	Low
Liability Rule	Low	High	Low	Low	High

*Table 2 (revisited): Features of Property versus Liability Rules*

As was suggested above, the analytic approach is a multi-factor evaluation of the relative import of these factors in the particular regulatory context, as well as the way in which any undesirable features of the legal rule-form could be addressed or ameliorated by using forms of legal preemption as well. The following provides a brief overview of each factor in Table 2 in this specific context.

*Flexibility.* As was noted in the discussion above, the importance of maintaining—and even improving—the great flexibility of the way web sites are designed and accessed cannot be understated. To be sure, there is today a general conception of what a ‘web site’ is, what it does, how it is built, maintained, and accessed: top-down, generally hierarchical sites; the collection of related information; the use of ‘pages’ to separate and hold content; the integration of text, images, and (sometimes) multimedia; internal linking between pages by the use of menus, etc. Perhaps even more strongly, there is a conception about the business model of providing web sites: mostly free access to all-comers; advertising revenue in some cases; an authentication-backed subscription model in rare cases. But these current conceptions of the ‘way the web works’ are just that—current conceptions. If there is anything that the history of the world wide web to date has taught, it is that its great value has been the huge array of experimental approaches that it has fostered. Many of these experiments have failed—spectacularly.<sup>147</sup> Others have succeeded.<sup>148</sup> And for some prominent players, the jury is still out.<sup>149</sup>

Recognizing the essential value of experimentation in this context suggests that the great danger in any regulatory effort here is to codify circa-2003 (or even earlier) thinking about the web. To no small degree, flexibility is what got

---

<sup>147</sup> Pets.com, Webvan.

<sup>148</sup> Yahoo!, eBay, Wall Street Journal Online.

<sup>149</sup> Amazon.com.



the web to its current point; any choice of legal rule-form must incorporate flexibility, or risk choking the progress of the online environment. This suggests that a property rule is strongly favored in this criteria.

*Institutional Intervention.* In some ways, the issue of institutional intervention seems somewhat less important in the web site access context than it might in an area where the models of information access and distribution are more complex. The World Wide Web is likely to be one area where regulatory institutions—the judiciary, regulatory agencies—have some level of familiarity, and thus one might be less concerned about this issue here. To the extent that institutional intervention is thought to be important, the reasons are likely to be derivative of other issues here: requiring institutional intervention implies a greater response time, or perhaps less flexibility (if the institution has a constrained view of the medium, for example). This factor appears to favor a property rule, though its import seems low.

*Response time.* Like flexibility, a fast response time seems to be particularly important in the cyberproperty context. This is not only because of changes in technology, but also because future changes in the way we think about the web, web sites, and networked information will necessarily require changes in access models. To this end, a legal rule supporting a faster rather than slower response time would seem to be broadly advantageous. Thus, this factor seems to favor a property rule.

*Transaction costs.* One of the unquestionable drivers of innovation in this context is the relatively low costs involved in building, developing, and maintaining a web site. (In some ways, of course, this obscures the fact that the huge quantity of web sites available mean that great costs are likely to be required to build traffic.) Thus, anything that would serve to greatly increase the costs of engaging in such development should be avoided. Indeed, concerns about transaction costs is perhaps the most-often invoked argument against property-type rules in the cyberproperty context.<sup>150</sup>

While transaction costs are at least a plausibly serious concern,<sup>151</sup> the choice of legal rule can fairly easily address it. It might do so in at least two ways.

---

<sup>150</sup> Burk, *supra* note 26 at 49; Hunter, *supra* note 5; Lemley, *supra* note 117.

<sup>151</sup> But see McGowan, *supra* note 26 at 23-25 (arguing that transaction costs will be low).

First, the establishment of a ‘strong’ default rule in favor of open access—i.e., one that requires meaningful notice to vary the default condition—will, as suggested above, greatly reduce the quantity of necessary transactions. That is, the expectation is that the vast majority of web access interactions will be on the basis of the default open access rule; only in the comparatively rare cases that vary from the default will any real ‘transaction’ be required. And second, as discussed further below, the legal rule can incorporate a (weak) form of legal preemption—requiring software mechanisms to be used for notice and transaction purposes. This should further reduce costs even for that small number of cases requiring transactions to alter the default rule.

In sum, transaction costs are an important criteria. As a general matter this should favor a liability rule, but there are important ways that even a property rule can be tailored or modified to greatly reduce the liability rule’s advantage on this criteria.

*Embedding Public Values.* At least three forms of ‘public values’ are invoked with respect to the web access issue. The first, and perhaps most cogent, is the great public value of the globally interconnected network—in the specific case of cyberproperty, the generally open access afforded to all Internet users.<sup>152</sup> The second public value is related to free expression principles: the ability of web developers to generally use web technologies (linking, access, etc) as part of their expressive purpose.<sup>153</sup> The third value is more closely related to competition issues: the concern that more variance in access requirements will allow some sites (especially commercial sites) to limit competition by imposing access requirements.<sup>154</sup>

There can be little doubt that there is great public value inherent in the Internet, and in widespread web site access in particular. The question is how much this impacts a choice of rule analysis. For if the assumption noted above is correct—that perhaps 85-90 percent of web developers affirmatively want open access to their sites—then there is good reason to believe that, given the appropriate default condition, the particular choice of legal rule won’t affect the vast majority of web sites. That is, if the default rule is one of open access, then even the imposition of a reasonably strong property rule-form shouldn’t have much impact on this 85 percent. This is even more the case if reasonable hurdles are established to change the default condition, such as clear notice

---

<sup>152</sup> Burk, supra note 26; Hunter, supra note 5; Lemley, supra note 117.

<sup>153</sup> See, e.g., Hunter, supra note 5, at 488-494.

<sup>154</sup> See, e.g., O’Rourke, Shaping Competition, supra note 26 at 1978-78.

requirements or the use of technological means to provide notice or facilitate transactions. And, as noted above, the effect on the remaining 10-15 percent of the sites is unclear; it may well be that the granting of a strong entitlement under a property rule will yield greater development, and thus more available information, even if the access rules are not fully open. Thus, while the values of the Internet are clearly important, it is far from clear how much such considerations affect the choice of a legal rule-form.

It is less clear that the other two expressed public values have as much special cognizance in the cyberproperty context, rather than raising general questions about the nature of property rights or the applicability of standard competition policy rules. Private entitlements often raise troublesome questions about their relationship to public interests in free expression; as a general matter, society deals with such questions by broadly allowing private rightsholders to enforce their rights under neutral laws without raising first amendment objections.<sup>155</sup> In some cases, narrow exceptions to property rules might be warranted.<sup>156</sup> In any event, as with the ‘global network’ argument, some of the concern can be diluted by the imposition of a default rule of open access and reasonable notice requirements. In similar fashion, the value of preserving competition is surely important, but seems to go more towards corporate behavior as measured by traditional competition policy principles rather than the choice of legal rule-form for a general cyberproperty entitlement.<sup>157</sup>

As a general matter, this prong seems to favor a liability rule, though perhaps less strongly when compared with a property rule incorporating the default condition noted above. (And even less strongly when compared to a property rule with some narrow exceptions.)

How one balances the factors above to determine a ‘final’ result is, as befits a normative analysis, a matter of considerable debate. Although the analysis above suggests with some force that a property rule may ‘edge out’ a liability rule in the specific context here, there is no doubt that the case is quite open; a reasonable policy analysis could come out the other way. The more important point is that, regardless of the outcome of the normative analysis, the inquiry is

---

<sup>155</sup> See, e.g., *Rowan v United States Post Office Department*, 397 US 501, 509 (1970); *Harper & Row, Eldred v Reno*. See also Epstein, *supra* note 26 at 86-87; McGowan, *supra* note 26 at 15-16.

<sup>156</sup> See, e.g., 17 U.S.C. § 107 (2001) (fair use).

<sup>157</sup> See, e.g., Sherman Antitrust Act of 1890 §§ 1-2, 15 U.S.C. §§ 1-2 (2004). See also McGowan, *supra* note 26 at 27-28 (doubting the possibility of widespread anticompetitive behavior in this context).

far from over. The normative decision must be considered in light of what Section IV above described as an instrumental inquiry: how does the choice of legal rule-form interact with the relevant software regulatory environment. It is this question to which the analysis now turns.

## 2. Hybridization in the Choice of Legal Rules

Section IV above demonstrated that choices of legal rule-forms cannot occur in a vacuum; they must incorporate an understanding of the rule's instrumental performance—the ability to affect the law-software interface—as well as address the policy option of a third rule-form: legal preemption, or the direct regulation of software effects.

Policy analysts will want to consider the instrumental performance of a legal rule-form for two reasons. First, if Section III is correct in noting the serious public-related concerns with software regulation, then there is significant value in choosing a rule-form that minimizes (or at least doesn't maximize) software regulation. Second, and irrespective of whether one believes the potentially negative effects of over-use of software regulation, Section II demonstrated that the net regulatory effects of a legal change will likely be unpredictable, absent consideration (and perhaps influence) of the software regulatory response.<sup>158</sup>

In the cyberproperty context, there is little to suggest that the general approach outlined in Section IV above does not apply. That is, an instrumental consideration of the choice of legal rules suggests that property rules are likely to perform significantly better than liability rules along this rubric, and that indeed, liability rules appear to be ineffective, except when paired with legal preemption rules.<sup>159</sup> This, then, suggests that the real analysis under the instrumental prong is among various forms of hybridization between traditional legal rules and legal preemption rules.

Indeed, it appears that the cyberproperty example offers a strong case for legal hybridization. There are a variety of potential software regulatory mechanisms available; while none seem attractive standing alone, the normative analysis above highlighted the possibility that such mechanisms might provide

---

<sup>158</sup> See *supra* Section II; see also text accompanying Figure 2.

<sup>159</sup> See *supra* notes 98-112 and accompanying text. Property rules are likely to perform better as they offer an attractive alternative to software—because of their potential strength (quantity of legal effects, to use the terminology above), and their greater flexibility. Liability rules generally contain neither feature, and are thus likely to be an unattractive alternative. See *id.*

important benefits. One promising option that springs out of the framework above is the combination of a property rule and a transactional form of legal preemption rule; that is, one having the following features:

- (a) Property rule: a rule that generally offers clear entitlements to injunctive remedies to web site owners for unauthorized access; and
- (b) Default condition: a default presumption in favor of open access, with nontrivial requirements of notice to vary this default; and
- (c) Legal Preemption (weak form): encouragement or requirement for the use of software techniques to implement any transactions that might be required.

This rule provides much of the benefits of a property rule, yet uses the default rule and legal preemption to reduce any transaction cost effects. Because it both provides a strong property rule and offers some legal preemption, it should stabilize the law-software interface by providing an attractive alternative to the various software regulation options noted in Table 4 above.

Note that this result is very similar to the current, albeit voluntary, practice related to the behavior of web ‘robots’ (or automated search indexers): a general default in favor of open indexing, with the use of a technological mechanism—the robots.txt file noted above—to change the default condition. It is also related to the result in *eBay v Bidder’s Edge*, which fundamentally upheld the access conditions established by eBay’s robots.txt file.<sup>160</sup>

This Section has applied the analytic framework developed in this Article to the particular regulatory challenge of cyberproperty. By integrating a detailed understanding of the software regulatory environment into the approach, a richer, more nuanced analysis was available. Consistent with the general observations, this Section suggests that in the cyberproperty context, an over-reliance on software regulation is likely to be socially detrimental. This fact then informs the choice of a legal rule-form, arguing in favor of a hybrid legal regime that has the basic attributes of a property right, tempered by both a default condition and a form of legal preemption.

This conclusion, however—that a hybrid property rule is best under these

---

<sup>160</sup> See *eBay v Bidder’s Edge*, *supra*.

Note also that Professors McGowan and Epstein reach a generally similar result, albeit via a different analytic path. See McGowan, *supra* note 26; Epstein, *supra* note 26.

particular circumstances—is necessarily conditional along a variety of dimensions. Consistent with a theme of this paper, as technological circumstances change, the analysis will almost certainly change as well. Furthermore, notwithstanding its multifaceted nature, the process followed here requires a number of balancing decisions—at least some of which could easily yield a different result. What is more important, however, is that the case of cyberproperty demonstrates both the challenges and the benefits of understanding the law-software interface.

## CONCLUSION

This Article has developed (and applied) a detailed analytic framework for the evaluation of regulatory policy in the cyberspace context. This new approach is in part a reminder of what cyberlaw has already taught—that both legal and software code have regulatory effects. But it is also an insight into lessons yet to be fully learned: that the intimate relationship between law and software in these modern regulatory environments demands a different, more complex and multidimensional, form of policy analysis. Law and software together define the regulatory condition; considering one without the other is fundamentally incomplete. Less law does not necessarily mean more freedom.

This deeply contextual inquiry into the relative (and additive) effects of law and software also reveals important limitations in software as a regulatory mechanism, suggesting that software compares poorly (at least from a public perspective) with legal regulation. Thus, an important aspect of regulatory policy analysis in this context is the extent to which the equilibrium between law and software is modulated appropriately.

And while the framework is necessarily highly dependent upon the context of any regulatory analysis—the specific technological and legal facts involved—it appears that in many cases property rules or those that directly relate to the corresponding software regulation (forms of legal preemption) will dominate. Flexibility in legal rules is paramount; traditional liability rules appear to be especially unsuited for this environment.

Considering the regulatory environment of cyberspace from the perspective of the framework of this Article may have profound effects on the way we think about the form and function of law in the modern regulatory environment. Indeed, the framework developed here is likely to have broad applicability to contexts beyond cyberlaw. As software (and thus regulation-by-software)

becomes increasingly ubiquitous in areas such as media creation and distribution and telecommunications, for example, the relevance of analytic processes that address both law and software will only increase. Software regulation is unquestionably here to stay. The real question is whether our policy approaches can meaningfully account for this trend, and whether the case against software will be fully understood.

APPENDIX A  
THE TECHNOLOGY OF SOFTWARE-ASSISTED CYBERPROPERTY

The specifics of the legal preemption recommended above could take a variety of forms. One general approach would use *metadata* embedded in web pages to specify (non-default) access and linking requirements. Metadata is information about other information; many forms of metadata are already in widespread use online. For example, “metatags” for the following descriptive features of a web page are common.<sup>161</sup>

Metatag	Description of Use	Syntax
Keywords	lists subjects of the web page, intended to assist web searching and indexing	<code>&lt;meta name="keywords" content="[...keywords...]"&gt;</code>
Description	describes the content of the web page, intended to assist in web searching	<code>&lt;meta name="description" content="[...description...]"&gt;</code>
PICS-Label <sup>162</sup>	describes the type and nature of content on a web page in code form; some web browsers allow users to block pages with certain attributes (e.g., ‘sexuality’ or ‘violence’)	<code>&lt;meta name="pics-label" content="[codes indicating the level of certain types of content]"&gt;</code>
Content-type	tells the web browser what specification the page is encoded for	<code>&lt;meta name="content-type" content="[codes indicating the level of certain types of content]"&gt;</code>
Expires	used for caching purposes; an ‘expired’ page is not served by the caching mechanism	<code>&lt;meta name="expires" content="[date and time]"&gt;</code>
Author	tags for the author of the content	<code>&lt;meta name="author" content="[author name]"&gt;</code>
Generator	tags for the software used to create the content	<code>&lt;meta name="generator" content="[software name]"&gt;</code>

---

<sup>161</sup> For a good general overview of the following metatags and the way they work, see Scott Clark, META Tag Tutorial, Webdeveloper.com, at [http://www.webdeveloper.com/html/html\\_metatags.html](http://www.webdeveloper.com/html/html_metatags.html). See also Scott Clark, META Tag Resources, Webdeveloper.com, at [http://www.webdeveloper.com/html/html\\_metatag\\_res.html](http://www.webdeveloper.com/html/html_metatag_res.html)

<sup>162</sup> See, e.g., W3C, Platform for Internet Content Selection (PICS), <http://www.w3.org/PICS/>



Metadata that described access and/or linking policies would then be available for a variety of automated or machine-assisted tasks. For example:

- (a) Web browsers could be configured to load only those pages with certain metadata, for example, ‘open-access’; or
- (b) Information about linking rights could be utilized by, for example, web development software packages or link-checkers to allow automated ‘clearance’ of linked-to sites.<sup>163</sup>

More sophisticated technologies could use metadata information to perform actual transactions:

- (a) Perhaps a \$0.0001 charge per page view of the Wall Street Journal Online could be deducted from one’s bank account; or
- (b) Web development software could report the conditions upon which linking is authorized—“only link to *Home*”; “only send 1000 hits per day”; “no traffic on Tuesdays”—which could of course be incorporated into modern dynamically created web sites.<sup>164</sup>

Obviously, none of this software currently exists; the point is that the basic building-block technologies do, and that given the appropriate incentives, one can expect this sort of technology to develop over time.

An outstanding example of the building of metadata technologies in a similar context is the *Creative Commons* project, which aims (in part) to facilitate automated or machine-assisted transactions concerning copyrighted materials.

---

<sup>163</sup> Link-checker software is commonly used to verify that all links (both internal and external) on a page are ‘live’ (i.e., working). It would be relatively easy to incorporate actions or reporting of such programs based on the metadata encountered.

<sup>164</sup> See, e.g., Phillip Greenspun, *Database Backed Web Sites: The Thinking Persons Guide to Web Publishing* (1997).