ON SOFTWARE REGULATION

R. POLK WAGNER*

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 equilibrium 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, how, and why concepts of property rights can be extended to bits stored on Web servers, e-mail 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.

* 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 of Pennsylvania Law School, and the Penn-Temple-Wharton Colloquium for helpful comments on earlier incarnations of this project. Ron Day, Kevin Goldman, Patrick Mirville, and Bill Mulherin provided research assistance.
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 better suited for a broad property rights regime than has been recognized to date.

TABLE OF CONTENTS

I. INTRODUCTION ........................................................................459

II. THE LAW-SOFTWARE INTERFACE: AN ANALYTIC FRAMEWORK ........................................................................465
    A. CODE MEETS LAW.................................................................466
    B. EQUILIBRIUM AT THE LAW-SOFTWARE INTERFACE..........468
    C. IMPLICATIONS OF CODE MEETS LAW I: DYNAMIC EFFECTS ................................................................470
    D. IMPLICATIONS OF CODE MEETS LAW II: UNPREDICTABILITY & UNCERTAINTY.....................................474

III. THE CASE AGAINST SOFTWARE: THE PUBLIC EFFECTS OF SOFTWARE REGULATION ................................477
    A. SOFTWARE AND REGULATORY SAFETY VALVES ....................479
    B. SOFTWARE AND THE RECOGNITION OF ENFORCEMENT COSTS ...............................................................480
    C. SCALING SOFTWARE................................................................481

IV. SOFTWARE AND THE CHOICE OF LEGAL RULES...............483
    A. PROPERTY RULES, LIABILITY RULES, AND LEGAL PREEMPTION .................................................................484
    B. CHOOSING THE FORM I: NORMATIVE ANALYSIS ..............488
    C. CHOOSING THE FORM II: INSTRUMENTAL ANALYSIS........493
    D. CHOOSING THE LEGAL RULE IN CYBERSPACE .................495

V. THE CASE OF CYBERPROPERTY.............................................496
    A. THE LEGAL-SOFTWARE LANDSCAPE OF CYBERPROPERTY....498
    B. THE LIMITED IMPACT OF A CYBERPROPERTY RULE AND THE IMPORTANCE OF DEFAULTS .................................502
    C. THE FLEXIBILITY IMPERATIVE ..............................................506
    D. THE PUBLIC GOOD OF NETWORK ACCESS .........................507
    E. CLARITY, STABILITY, AND CERTAINTY ...............................508
    F. CHOOSING AMONG FORMS OF LEGAL REGULATION........508

VI. CONCLUSION...............................................................................516

VII. APPENDIX .....................................................................................517
I. INTRODUCTION

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.\(^1\) Code is law; architecture is control; software is power.

While there is no question that the basic point made above is correct, it is nonetheless the case that widespread acceptance of the “code is law” meme has obscured the kaleidoscopic relationship between legal code and software code.\(^2\) 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.\(^3\) As Lawrence Lessig stated:

In real space we recognize how laws regulate—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.\(^4\)

---


3. See, e.g., LESSIG, CODE, supra note 1, at 6; Boyle, supra note 1, at 182; Katsh, supra note 1, at 340; Lessig, Horse, supra note 1, at 503; Reidenberg, supra note 1, at 554–55.

4. LESSIG, CODE, supra note 1, at 6.
This insight into the power and importance of software code in this context has become both widely discussed and broadly accepted. Its implications are disputed: some commentators, most prominently Lessig, suggest that technology—harnessed by commercial interests—is likely to substantially limit freedom in cyberspace; 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.” Still others, while not disagreeing with the central code-is-law point, inquire as to whether it raises much of an issue at all.

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, 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, and so on. 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. The concept’s import in cyberspace comes from the uniquely mutable nature of the computer technology that forms the online world. 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 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

6. See LESSIG, CODE, supra note 1, at 6.
7. Wu, supra note 2, at 681.
9. Indeed, a July 2003 search in the LEXIS ALR database using the following query returned 759 hits: “code is law” and (software OR technology OR internet OR cyberspace).
10. See, e.g., LESSIG, CODE, supra note 1, at 86–90.
11. See Lessig, Horse, supra note 1, at 506.
directly interchangeable with law, and it is easy to understand how the regulatory mechanisms differ. 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. Nobody, for example, seems to argue directly that any particular snippet of software can directly replace 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. 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. 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 shape the emerging regulatory infrastructure of cyberlaw.

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

12. See id. at 509–10.
13. Indeed, Lessig in particular presaged this line of analysis, noting that what he called “modalities of regulation” would both compete and interact. See id. at 508–10. See also Lawrence Lessig & Paul Resnick, Zoning Speech on the Internet: A Legal and Technical Model, 98 MICH. L. REV. 395 (1999).
14. Tim Wu has recently asked a similar question, noting that software code can at times be used to avoid or mitigate the effects of legal rules. See Wu, supra note 2. As noted below, this observation fits well into the analytic structure derived here. See infra note 34 and accompanying text.
15. See, e.g., LESSIG, CODE, supra note 1, at 6–8; Lessig, Horse, supra note 1, at 512.
16. See LESSIG, CODE, supra note 1, at 6–8; Lessig, Horse, supra note 1, at 513. Patricia Bellia has recently made a similar set of points. See Patricia L. Bellia, Defending Cyberproperty, 79 N.Y.U. L. REV. 2164 (2004).
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 on the interactions along the law-software interface. Similarly, changes in the technological (software) environment will advance responsive changes in legal rules, yielding perhaps more or perhaps less regulation, under different circumstances. 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 of 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. Indeed, in many cases, the response may be difficult to predict ex ante, meaning that the net regulatory effects are likely to be unclear. 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. 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 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 attractive alternative to legal regulation can have troubling public effects, at least compared to legal regulation. Software regulation lacks forms of

17. Lessig makes a related point. LESSIG, CODE, supra note 1, at 206 (arguing that the absence of law “will cause a shift in effective regulatory power—from law to code, from sovereigns to software”).
18. See infra Part II.A.
19. See infra Part II.A.
20. See infra Part II.D.1.
21. See infra Part II.C.
22. Note that this constitutes 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, and indeed likely do not, have the 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 65–66 and accompanying text. Thus, these concerns
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 overuse of software regulation will yield a regulatory environment that is at once more extreme and less stable than that which incorporates 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.23

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.24 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 rules containing forms of legal preemption.25

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.26 In stepping through the analytic framework

---

23. See infra Part III.


25. See infra notes 109–112 and accompanying text.


For academic treatments, see, for example, Dan L. Burk, The Trouble with Trespass, 4 J. SMALL & EMERGING BUS. L. 27 (2000); Niva Elkin-Koren, Let the Crawlers Crawl: On Virtual Gatekeepers
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 or transactions (or both). 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 overreliance 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.

What follows has four parts, beginning, in Part II, with an 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.

Part 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, Part 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.

Part 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. Part VI provides a brief conclusion.

II. THE LAW-SOFTWARE INTERFACE: AN ANALYTIC FRAMEWORK

This part provides a basic analytic framework for thinking about the relationship between the two major regulatory modes of cyberspace noted above, law and software. This construct emerges from the observation that the law-software relationship in cyberspace is primarily defined by complementarity rather than substitutability, or is fundamentally additive rather than subtractive. Put more simply, for a given regulatory condition, the impact of law—cases, statutes, and so on—will deeply influence the impact of software. Indeed, the idea here is to think in terms of equilibrium, 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, point 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 overreliance on software-regulatory techniques as a policy lever will be counterproductive. A close look at the

27. 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, is that between law and software, the effects of norms and the market will be noted less systematically, though their most important effects will be described.
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. The more pressing inquiry relates to the nature of the law-software relationship and its effects on the behavioral infrastructure of cyberspace. 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 regulatory effects and software-regulatory effects.

28. The normative implications of this phenomenon, however, are controversial. See supra notes 5–8 and accompanying text.

29. See, e.g., Wu, supra note 2, at 680–82.
Figure 1, below, depicts the basic point here graphically.

**FIGURE 1.** The law-software interface

![Diagram](image)

Here, the axes represent the effects (or impact) of the two regulatory modes, law (y-axis) and software (x-axis). 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 software effect (here, 2). In the Figure 1 construct, the equilibrium condition is depicted as point a (2,4), and the total regulatory effect is designated as $2 \times 4 = 8$.

---

30. To be complete, Figure 1 should encompass four dimensions, corresponding to law, software, norms, and the market, respectively, and each having regulatory effects. *See* LESSIG, CODE, *supra* note 1, at 165. The author, however, found it problematic to describe graphically the more encompassing relationship.
Less abstractly, and using the cyberproperty example central to this Article, regulatory Condition A can be said to represent the total excludability that owners of Internet-connected resources (Web servers and e-mail systems, among others) enjoy—that is, the content of the cyberproperty right. That quantum of regulatory effect (again, designated as \( A \) here) is the product of both legal protections—perhaps state-backed property-type rights (doctrinally, a remedy for trespass), and software-constructed protections, such as link-denial code, password protections, or others.

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. 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.

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- and antiprotection effects, the Copyright Act both provides legal protections and sets limits on the amount of protection provided. 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-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 conditions will provide a legal response.

---

31. As I note in the discussion in Part II.D below, the uncertainty associated with the existence, scope, and nature of the legal protections for the cyberproperty right has important policy consequences.

32. See Part III below for a detailed look at the software-regulatory options.


34. The canonical example, and the one discussed in detail by Wu, is peer-to-peer software products, which allow for the easy—and only partially susceptible to regulation—exchange of copyrighted goods (typically music or movies) between network users. Wu, supra note 2, at 726–45.

35. Compare 17 U.S.C. § 106 (detailing a copyright owner’s exclusive rights in a copyrighted work), with id. § 107 (detailing the fair use defense to unauthorized use of a copyrighted work).
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. There are of course tremendously important public effects and responses, as discussed in Part III below; the point of the analytic framework here is to describe the impact of private decisionmaking 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 his or 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 perhaps 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 are triggered only after a violation arises, which may offer less protection in the dynamic Internet environment.

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 Web site owners with a choice concerning whether to deploy software-based regulatory mechanisms. For example, they could implement a link-blocking mechanism based on the hypertext transfer protocol (“http”) that is

---

36. It also represents average behavior. Obviously, in the absence of explicit restrictions otherwise, see infra text accompanying note 45, individual responses to legal effects will vary. The figures here are intended to convey the overall average response rather than suggest that all players will behave the same.

37. 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, causing either a crash that resulted in at least temporary downtime or greatly slowed access to the site, an ex post remedy would seem pyrrhic; though if monetary damages could be calculated, they might, at least in theory, be recovered. Similarly, the possibility of an injunction against future unwanted links might be useful in some cases.
intended to allow traffic only from designated referring Web pages. The use of this technique will 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. Ultimately, deployment will depend on 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.

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; 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) stronger legal regulations and have yielded new litigation tactics calculated to increase the net effects of the copyright law. Again in Figure 1 terms, this moves point \( a \) upward, indicating a greater legal regulatory effect—and thus greater overall regulatory conditions, assuming stable software effects.

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 straightforward of these observations is that the law-software interface is
profoundly dynamic in the cyberspace context. 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 long term) yield changes in the other. 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 (or paradigmatically to legal scholars, as 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: as noted above, it is the product of law and software effects that determine the overall regulatory environment.

43. 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.

44. 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 systems, one can expect these transitional effects to have more significance in slowing legal changes in response to software developments than vice-versa.
Consider, for example, Figure 2, depicting changes in conditions.

Figure 2 describes a change in legal regulatory effects (a decrease from 4 to 2, as when the law reduces or eliminates 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; the appropriate software may not meaningfully exist, or it is too inflexible to be useful, for example. In this case, total regulatory effect reduces from an 8 in Condition A (2 x 4) to 4 in Condition B (2 x 2). Given a utilitarian model, one would thus expect a change in the output or development of the protected/regulated good in Condition B. This could be either a positive or negative change, depending

45. Another possibility for Condition B, which I discuss more fully below, see infra notes 87–96 and accompanying text, is that the legal regulation directly implicates the software regulation, perhaps by preempting or discouraging certain software deployments.
on a variety of assumptions about the development environment. For purposes of the illustration 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 and development.

Condition D illustrates an increase in software effects of a magnitude that renders no net change in the regulatory environment. Here, law and software are fungible, at least from a net regulatory effects perspective. (As discussed in Part II.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: the reduction in legal effects prompts a technological response of such magnitude that it actually increases the overall regulatory effect. This could occur, for example, if the increase in resources devoted to research and development (“R&D”) of software-regulatory techniques (spurred by the drop in legal effects) yielded a breakthrough in cost effectiveness, allowing greatly increased deployment of software mechanisms. Perhaps a reduction in the legal force of copyright law spurred R&D into DRM systems that enabled huge advances in effectiveness to be made. 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 increased use of password-protected (or otherwise individually restricted) network resources. Given the change in overall regulatory effect (an increase to 10 (5 x 2)), Condition E will also feature

---

46. An example might be “unbreakable” DRM systems, or even copy-protected CDs that work reliably.

47. 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 were such that Web site owners who wished to prevent unwanted access were required to use the 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.
output and development effects in the opposite direction from those resulting from Conditions B and C.

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 reuse of copyrighted materials by expanding the notion of fair use—a proponent would undoubtedly be 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 of law and software demands careful consideration of each. Code is not equivalent to law, a point that 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 explore 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 caused by legal decisions. Second, given the rapid development of software technologies in recent years, especially in the cyberspace context, 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. 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.

The 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 or seamless (and borderless) data file transfer, are now commonplace. The costs (and complexity) of publishing oneself in cyberspace has plummeted rapidly. And yet still one gets the sense that only the tip of the iceberg is 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. 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 cyberspace. Software is a constantly updated

---

49. 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. See Gordon E. Moore, Cramming More Components onto Integrated Circuits, ELECTRONICS, Apr. 19, 1965. This observation has more or less held true since it was first noted in 1965 (although Gordon Moore’s original prediction was actually a slightly more optimistic doubling every year). See John Markoff, Is There Life after Silicon Valley’s Fast Lane?, N.Y. TIMES, Apr. 9, 2003, at C1. Moore has recently suggested that the “Law” is likely to hold true for some period into the future. See Gordon E. Moore, No Exponential is Forever . . . but We Can Delay ‘Forever,’ Presentation at the International Solid State Circuits Conference (Feb. 10, 2003), at ftp://download.intel.com/research/silicon/Gordon_Moore_ISSCC_021003.pdf.
50. See Peter Grant, Miss the Final ‘Sopranos’? Getting Cable TV on Demand, WALL. ST. J., Dec. 12, 2002, at D1; Seth Schiesel, Video on Demand Is Finally Taking Hold, N.Y. TIMES, Nov. 25, 2002, at C4.
51. See Wu, supra note 2, at 683, 717–19 (describing peer-to-peer software technologies).
52. Take, for example, Web logs.
53. See generally LESSIG, CODE, supra note 1.
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—55—and revolutionary—moving in sudden leaps ahead.56 The result is a trend line 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.57 And yet the last several months have shown an explosion of activity surrounding Web logs (or blogs) as an innovative medium for communications,58 as well as the advent of viable Web-based models of music distribution.59 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 lead to dramatic increases in impact once a critical level of adoption or deployment is reached.

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

55. 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); Apple Computer, Mac OS X: Based on Unix, at http://www.apple.com/macosx/technologies/darwin.html (last visited Jan. 5, 2005) (describing the UNIX underpinnings of its most modern operating system, Mac OS X); Lucent Techs., The Creation of the UNIX Operating System, at http://www.bell-labs.com/history/unix/ (last visited Jan. 5, 2005).


59. See, e.g., Sarah McBride, Virgin Group Plans New Venture to Enter Online Music Business, WALL ST. J., Mar. 8, 2004, at B4 (reporting that online music sales are estimated at $200 million). 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, at C4 (“Apple makes little or no profit from each song downloaded, [but sales of digital music players] . . . were crucial to Apple’s financial resurgence.”).
actors, who are both unlikely to have personal skills related to software development and are less likely than legislatures to become more informed. 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 equilibrium would appear to be quite temporary. For example, only relatively minor forms of DRM seem to exist presently in the music context; 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. 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. These instability effects again suggest that overreliance on software as a significant component of the regulatory infrastructure is likely to be problematic.

This part has established an analytic framework for the interrelated regulatory effects of legal and software code, emphasizing both the complex and contextual nature of this relationship. The remaining parts 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 is that policy initiatives in cyberspace demand consideration of both legal and software effects. That is, if both law and software are regulatory, and the

60. Absent direct (legal) regulation of software effects.
62. See, e.g., Steve Pain, MS May Have the Answer to Piracy, BIRMINGHAM POST, Jan. 28, 2003, at P21.
63. Lessig appears to share this concern as well. See Lessig, Horse, supra note 1, at 529.
status of each determines overall regulatory effects, then an important consideration in any policy analysis is the mixture between the two. It is unquestionable that law and software regulate in different ways. This fact implies that each has different public effects. This part explores the public effects of regulation by software, informing the detailed policy analysis required in the cyberspace context.64

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 Laws 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,65 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 differs sharply from law as a mechanism of regulation.66

At least some of these differences suggest that, irrespective of the cost-effectiveness calculations explained in connection with 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 are described below.

*Preprogrammed.* Software regulation operates in a relatively fixed, rigid fashion in determining 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, an 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 narrow—range of inputs in implementing the regulatory rules. The quantity, scope, and nature of these inputs are often

---

64. Bellia has recently made related points on the importance of considering both legal and technological components of regulation. See Bellia, *supra* note 16, at 2164–65.


66. Lessig appears far less concerned about the spread of open-source developed software code, which attenuates the ability of private commercial actors (or, indeed, the government) to meaningfully control it. See *id.* at 100–08; Lessig, *Horse, supra* note 1, at 536–38.
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 communication, has a relatively small number of fields (headers) that offer information about users that would allow determinations to be made concerning the authorized use of network resources.67

Self-contained. The point here is obvious: software-implemented regulations are freestanding mechanisms68 and do not generally require recourse to other institutional players for enforcement and rule determinations. This contrasts with more typical legal regulation, which generally requires recourse to other institutions or players—courts, arbitrators, prosecutors, regulatory bodies—for decisionmaking related to enforcement.

Marginally costless. Software-regulatory operations are generally unaffected by the quantity of use.69 A well-designed authentication or link-blocking system will be able to block a single unwanted request per 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. This broad, public-oriented view of software may have negative implications, however, that should give pause to proponents of software. The sections that follow discuss these implications in brief.

A. SOFTWARE AND REGULATORY SAFETY VALVES

Even under legal schemes that demand little or no intervention on the part of third-party regulatory institutions, such as property-backed

67. Most important among these are the “referrer” 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.

68. This is not to say that software regulation will not access external resources, such as databases, for information or assistance. Rather, the observation is that software mechanisms inherently combine information collection, rule analysis, and enforcement.

69. They are free standing at least to a point. There are of course capacity constraints in any system, the violation of which can trigger a number of problems.
contracts, there nonetheless exist a number of “safety valves” that ensure that private arrangements conform to acknowledged boundaries of social practice. These safety valves can be explicit; examples include the doctrine of unconscionability in contract law (which serves to ensure that agreements are entered into voluntarily), unfair competition law (which serves to ensure that private dealings do not stifle the functioning of the market), or even broader social values, such as principles of nondiscrimination. Or they can be less formal, such as the restraint encouraged by public enforcement of contract law, which may subject the author to unwanted publicity.

By obviating the need to seek recourse from third-party enforcement institutions—such as courts or regulators—software regulation can “fly under the radar,” avoiding the oversight, both formal and informal, that occurs in even 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—specifically 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. Another example is an access blocking mechanism that blocks 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 antiregulatory 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 Web surfing, for example.

B. SOFTWARE AND THE RECOGNITION OF ENFORCEMENT COSTS

It is axiomatic that the enforcement of legal rights will not 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 be beneficial in many cases; 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.\footnote{For further discussion on this point, see generally R. Polk Wagner, \textit{Information Wants to Be Free: Intellectual Property and the Mythologies of Control}, 103 COLUM. L. REV. 995 (2003).}

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 do not exist—and the effects noted above will not be realized.\footnote{ Accord Bellia, \textit{ supra} note 16, at 92–93.} Again, two implications seem especially relevant. The first is the loss of the beneficial effects of recognizing 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. This breeds potential for instability and demoralization, similar to the situation where safety valves are absent.

\section*{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. However, 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;\footnote{ This situation is exacerbated by an institutional tendency to underreport potential defects at the performance testing stage prior to release. \textit{See}, e.g., H. Jeff Smith & Mark Keil, \textit{The Reluctance to Report Bad News on Troubled Software Projects: A Theoretical Model}, 13 INFO. SYS. J. 69 (2003); Lisa Liberty Becker, \textit{Telling the Truth Can Be Hazardous to Your Job}, BOSTON GLOBE, Apr. 6, 2003, at G9. \textit{See generally NAT’L INST. OF STANDARDS & TECH., U.S. DEPT. OF COMMERCE, THE ECONOMIC IMPACTS OF INADEQUATE INFRASTRUCTURE FOR SOFTWARE TESTING (2002).}} 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 countermeasures.\footnote{ \textit{See}, e.g., Christopher Jones, \textit{Internet Hacking for Dummies}, WIRED NEWS, Feb. 20, 1998, at http://www.wired.com/news/technology/0,1282,10459,00.html (last visited Jan. 5, 2005). 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.’” \textit{ERIC S. RAYMOND, THE CATHEDRAL AND THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY} 41 (1999). \textit{See also} Yochai Benkler, \textit{Coase’s Penguin, or, Linux and The Nature of the Firm}, 112 YALE L.J. 369, 434–36 (2002).} Further, software regulation is unlikely to fail gracefully. Once bugs or countermeasures are
discovered, the effectiveness of the particular regulatory mechanism is substantially diminished. 74 This phenomenon—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 (that is, 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 is worth, especially as the number of agreements rises rapidly. 75 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 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.


Additionally, efforts to repair vulnerable or defective software systems are typically problematic. See George V. Hulme, Companies Pay Up to Plug Holes, INFO. WEEK, May 20, 2002 (noting that hackers outpace the repair efforts of security administrators), at http://www.informationweek.com/story/showArticle.jhtml?articleID=6502382; Douglas Schweitzer, Emerging Technology: Patch Management—Patch Me If You Can!, NETWORK MAG., Aug. 1, 2003, at 40 (noting that 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.

IV. SOFTWARE AND THE CHOICE OF LEGAL RULES

The preceding two parts 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 part 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.76

A key observation here is that the choice of legal rules in cyberspace is not just a choice between the classic dichotomy of “property rules” and “liability rules” (and mixtures thereof), but it is 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.”77 That is, given the analysis in Parts II and III, the choice of legal rule in this context has a traditional normative component (that is, which form of legal rule provides the best or most efficient regulatory mechanism?), and a distinctly instrumental component (that is, 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.

76. As Tim Wu importantly suggests, some groups may find software to be a more convenient approach to altering the regulatory landscape. See Wu, supra note 2, at 683, 717–19 (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.

77. The description of property rules and liability rules as defining the basic forms of legal rules was established in Guido Calabresi and A. Douglas Melamed’s seminal article, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral. Calabresi & Melamed, supra note 24, at 1092.
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. A property rule grants the rights holder, 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 and terms of use). 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. Again, in the cyberproperty context, a liability rule would grant access subject to harmful acts that would trigger liability—for example, extreme overuse of bandwidth or forms of linking bordering on misappropriation.

It is widely argued that, following Coasean 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. Where transaction costs are high, or bargaining is not possible, however, liability rules are the better choice.
Yet the binary choice of legal rule-form is fundamentally incomplete in the cyberlaw context. 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. 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. 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.

There are several possible forms of this regulatory technique, ranging generally from strong to weak. 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 (“AHRA”) 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. 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.

Another, somewhat less strong form is regulatory standardization, where legal regulations establish the framework within which software will operate. For example, the Federal Communications Commission (“FCC”)

85. Abraham Bell and Gideon 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 exists, which they describe as “pliability rules.” See Bell & Parchomovsky, supra note 78, at 5. To some degree, the hybrid forms of traditional legal rule-forms and legal preemption described here are related to their concept of pliability rules.

86. See supra Part II.

87. Lessig describes this phenomenon as “law regulating code.” Lessig, Horse, supra note 1, at 532–34.


has established the technical standards for digital television. 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. 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. Note that, while counterintuitive, 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 is reached, there will be diminished incentives to seek stronger software effects, given that no additional legal protection will be 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 utilize the P3P standard, or that Web pages are to be tagged according to the PICS standard to allow for content

92. See Wu, supra note 2, at 708–26 (describing the effects of anti-regulatory code in changing the regulatory condition for copyrighted goods).
94. 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/ (last visited Jan. 5, 2005).
filtering and selection; each has a comparatively small regulatory component, its chief aim being to establish a transactional framework.

Table 1 summarizes the spectrum of legal preemption.

**TABLE 1. Forms of legal preemption rules**

<table>
<thead>
<tr>
<th>Strong Forms</th>
<th>Weak Forms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct</td>
<td>Transactional</td>
</tr>
<tr>
<td>Standardization</td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td>P3P or PICS mandate</td>
</tr>
</tbody>
</table>

| AHRA | FCC activities | DMCA |

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 is this: just as the choice of a legal rule will involve analytic trade offs between the familiar categories of property rules and 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).


96. Of course, as any lawyer will note, even transaction or procedural rules have substantive effects. Thus, transactional forms of legal preemption rules will have some regulatory effects. The point here is to try to tease out some general distinctions for more fine-grained policy analysis.
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 compare 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 Parts II and III above, as operating both to establish a legal regulatory effect (that is, protection or entitlement) and to generate a software-regulatory response, the choice of form analysis includes both
normative and instrumental components.\textsuperscript{97} The normative component of the analysis is well understood. It asks: which legal rule is most likely to provide the desired legal effects?\textsuperscript{98} The instrumental component considers the legal rule in the context of its impact on software regulation, and asks which rule-form will be most effective at influencing the software response. Each of these evaluations must be conducted for each dimension of regulation (see Figure 3)—property versus liability rules, and strength of legal preemption.

1. Property Rules Versus Liability Rules

The first step is to reevaluate 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.\textsuperscript{99} Instead, the analysis focuses on those factors that appear to take on heightened relevance in the cyberlaw context and evaluates how they play out. Thus, the analysis is to a degree 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 (as a result of technological changes) and very complex interactions between the legal rules and software techniques.\textsuperscript{100} This suggests that three factors in particular are especially relevant. First among them is 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 described in Part II above, the ability to dynamically respond to changing conditions is important to stability in the regulatory environment. Therefore, 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 significant costs in uncertainty and errors resulting from additional (and customary) institutional intervention.\textsuperscript{101}

\textsuperscript{97} See supra notes 45–47 and accompanying text.
\textsuperscript{98} See Calabresi & Melamed, supra note 24, at 1090–93.
\textsuperscript{99} See id. at 1106–10.
\textsuperscript{100} See supra notes 43–47 and accompanying text.
\textsuperscript{101} See McGowan, supra note 26, at 343, 357–58.
A third factor is the responsiveness of any legal rule. As described above, changes in the software-regulatory context can dramatically alter the overall regulatory condition.\textsuperscript{102} 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.\textsuperscript{103} 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 rule will be significant, due to the huge multiplier effect of the number of transactions conducted, or potentially conducted, online.

The last relevant factor is the question of embedding public values—such as free speech, diversity of opinion, and privacy—into the regulatory construct.\textsuperscript{104} 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. 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 and enhance diversity, expression, and individualism.\textsuperscript{105} And while there is at least some doubt as to its heightened importance in the cyberlaw context, this is a widely held view, and thus should be included in the analytic process.\textsuperscript{106} Here, a liability rule, by allowing more control over

\textsuperscript{102} See supra notes 36–42 and accompanying text.
\textsuperscript{103} See, e.g., Bell & Parchomovsky, supra note 78, at 3–4; Calabresi & Melamed, supra note 24, at 1103.
\textsuperscript{104} See, e.g., Lessig, Horse, supra note 1.
\textsuperscript{105} See, e.g., LESSIG, CODE, supra note 1, at 8. See also Elkin-Koren, supra note 26, at 195–208 (exploring the role law may play in ensuring a competitive search engine market); O’Rourke, Shaping Competition, supra note 26, at 1978 (arguing that product differentiation “is not a strong basis for granting control over product and pricing information to a web site”).
\textsuperscript{106} The counterarguments take one of two forms. The first questions the premise of Internet exceptionalism that underlies many arguments related to the great public import of the Internet. Surely the Internet 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 (that is, equality and social entitlements). See Easterbrook, supra note 8; Goldsmith, supra note 8.

The second response generally accepts the Internet exceptionalism premise, while suggesting that the best way to maximize the Internet’s potential is to leave the decisions in the hands of private individuals. This response emphasizes that much (if not most) of the explosion related to the Internet is the result of private decisionmaking (sometimes, but not always motivated by profit), and that absent serious indicators otherwise, government interference should be minimized. See Wagner, supra note 70.
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.

TABLE 2. Features of property rules versus liability rules

<table>
<thead>
<tr>
<th>Rule-Form</th>
<th>Flexibility</th>
<th>Institutional Intervention</th>
<th>Response Time</th>
<th>Transaction Costs</th>
<th>Embedding Public Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property Rule</strong></td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Liability Rule</strong></td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

Whether one is convinced that the results displayed in Table 2 point strongly toward a particular form of legal rules will depend largely on a normative judgment about the relative importance of each factor. In this sense, the analytic process is much like a more traditional choice of legal rule-form.\(^{107}\) 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 (that is, regulatory issue), certain factors may be deemed more important than others. For example, the argument in Part V.C 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.\(^{108}\)

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. 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.

---

\(^{107}\) See Calabresi & Melamed, *supra* note 24, at 1103.

\(^{108}\) See *infra* notes 147–157 and accompanying text.
2. Strength of Legal Preemption

As noted above, the goal of a rule of legal preemption is fixing (or influencing, in weaker form) the corresponding regulatory effects of software.\textsuperscript{109} Therefore, the series of concerns raised regarding the use of software as a regulatory mechanism suggests 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 the limitations 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 Part II above, software development is a rapidly moving, nearly unpredictable target, making it difficult to directly address software through legal regulation.\textsuperscript{110} It is not impossible, certainly, but difficult as a technical matter because, 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 this point of difficulty, 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 level of legal protection in the cyberspace context that is too low may be partially overcome by the effects of software regulation. The combination of both too little law and direct software regulation (of the preemption form, perhaps) would be far more problematic, however. For example, serious problems could arise if the legal regulation encompassed more forms of software than intended, thus resulting in serious unintended consequences. Indeed, this is an oft-heard criticism of the DMCA: that its scope is such as to encompass business practices\textsuperscript{111} and even bona fide research\textsuperscript{112} well outside the support of basic DRM systems.

\textsuperscript{109} See \textit{supra} notes 78–96 and accompanying text.
\textsuperscript{110} See \textit{supra} notes 49–63 and accompanying text.
Finally, the question of direct regulation of software raises questions of institutional competence. As noted above, there are reasons to think that courts are not well suited to engage in meaningful software-regulatory policy analyses. Legislatures or regulatory bodies might have a better chance, but the rapidly developing environment suggests that any move to take the path and pace of software development away from private decisionmakers is one that must 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 that, as discussed above, the various forms of legal preemption rules raise differential concerns; as a general matter, the weaker, less interventionist forms of legal preemption are less likely to have problematic side effects. In any event, it seems 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 Part 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. This section steps through the analysis of the instrumental effects of the choice of legal rule.

1. Property Rules Versus Liability Rules

As noted in Part II above, absent direct regulatory effects (legal preemption), the law-software equilibrium for a particular regulatory condition is generally determined by private decisionmaking related to the costs and 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 rights holders the ability to set restrictive conditions for access—even quite stringent ones—without the need to resort to software regulation. A liability rule is, by definition, 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 rights holders, it is less likely to discourage the use of software regulations.

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

Here, both the potential strength of the legal effects and the flexibility in arranging rights strongly suggest that a property rule 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 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 with which a legal rule influences the law-software equilibrium—the advantage is manifest: a rule including legal preemption will, by definition, have significant effects on the law-software interface. Depending on the level of intervention, these effects can range from almost complete determination of software regulations to indirect encouragement.

There are significant potential downsides. First, legal preemption requires a trade off between the advantages inherent in software regulation—particularly flexibility—and the effectiveness of the rule in

113. See Epstein, supra note 26, at 84 (noting the particularization and standardization achievable in contractual agreements); McGowan, supra note 26, at 373.
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 flexibility, but they will have more attenuated effects.

A second important concern, related to the first, is that the use of legal preemption increases the costs of error inherent in regulatory decisionmaking. Assume for the moment two legal rules in the cyberspace environment, each establishing the same legal effect X (that is, the same amount of legal protection). The first is a traditional legal rule, one without preemption. The second is a rule including strong legal preemption aspects. If the quantum of legal effect X is somehow inappropriate or erroneous—perhaps the protection is too weak to support the development desired, or is too strong, given public policy considerations—then one can expect the regulatory environment in the first case to adapt, at least to 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. 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 increases the chances for costly (or even enormously costly) errors.

D. CHOOSING THE LEGAL RULE IN CYBERSPACE

This part 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 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 affect 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 is that the decisionmaking criteria must be expanded to incorporate the instrumental effect of legal rules. Indeed, if one agrees with the analysis in Part II above, namely that, in many cases, software regulation is a poor substitute for legal regulation, then instrumental performance may be as important as the more traditional normative analysis of a legal rule-form.
Although the choice of legal rule-form is revealed to be deeply complex and contextually dependent on legal and technological circumstances, there are a few general observations that spring forth. The first is that “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 supported by 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 how this modern environment enables the mixing of forms of traditional legal rules (property and 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 to address the concern about transaction costs that attach to property rules. In addition, such hybrid rules suggest that careful policy analysis can tailor legal rule-forms to address the particulars of a given regulatory context in cyberspace.

V. THE CASE OF CYBERPROPERTY

This part applies 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. For example, a cyberproperty right will allow owners to determine the details of the use of their Web sites, e-mail 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 part is intended to conceptually encompass a range of emerging and related legal actions, each with different doctrinal foundations. This range of doctrinal approaches, along with a few of their important features and regulatory effects, are

114. I recognize that the invocation of the term “property” here suggests an analogical connection between access protections online and those in realspace—that is, real property. As should become clear below, however, this analysis does not place weight on real property premises.

115. Table 3 below notes the variety of legal sources from which the cyberproperty entitlement might be said to emanate. Taken collectively, these recent legal developments constitute 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 Burk, supra note 26; Elkin-Koren, supra note 26; Epstein, supra note 26; Hardy, supra note 26; McGowan, supra note 26; O’Rourke, Analogy, supra note 26; O’Rourke, Shaping Competition, supra note 26.
described briefly below. The goal of this part, however, is not to engage in
the sort of detailed doctrinal analysis that has been an important part of
earlier contributions, nor to suggest new doctrine that better establishes the
cyberproperty right. Instead, the purpose here is to use the regulatory
confusion surrounding this important question as a hook on which to hang
a broader form of policy analysis, following the lessons of the discussions
above.

It is clear that, whatever the current state of cyberproperty, the issue of
rights of access in cyberspace is hotly contested. In particular, the trespass
to chattels approach to this issue has been hotly contested among legal
scholars recently—especially doctrinally—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 of search engines, as well as to describe the current state of
affairs as “nothing short of disastrous as a matter of public policy.”
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.

The analysis in this part 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 include the
following:

(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;

116. See Burk, supra note 26; O’Rourke, Analogy, supra note 26.
117. See Brief of Amici Curiae in Support of Bidder’s Edge, Inc. at 8–10, eBay, Inc. v. Bidder’s
jurist.law.pitt.edu/amicus/biddersedge_v_ebay.pdf (last visited Jan. 5, 2005).
119. See Epstein, supra note 26; McGowan, supra note 26.
(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 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 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 consider the cyberproperty right in terms of its specific application to the World Wide Web—that is, access to Web sites and servers. Similar analyses would be appropriate for related applications involving other network-connected resources, such as e-mail systems.

A. THE LEGALSOFTWARE LANDSCAPE OF CYBERPROPERTY

Consistent with the analytic framework developed in Part II of 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”). Table 3 outlines the basic features of these doctrines, and considers the scope of their legal effects.

TABLE 3. The legal environment for cyberproperty

<table>
<thead>
<tr>
<th>Doctrine</th>
<th>Protection</th>
<th>Key Case</th>
<th>Regulatory Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trespass to Chattels</td>
<td>Unauthorized access to physical servers</td>
<td>eBay, Inc. v. Bidder’s Edge, Inc.¹２¹</td>
<td>Medium: relatively strong, though doctrinal uncertainty concerning damages</td>
</tr>
<tr>
<td>Copyright Law</td>
<td>Possible protection of certain forms of inline linking</td>
<td>Kelly v. Arriba Soft Corp.¹²²</td>
<td>Unclear: serious questions of applicability to this context; fair use defenses exist</td>
</tr>
<tr>
<td>(Naked) Contract Law</td>
<td>Implementation of TOS agreements posted on page</td>
<td>Register.com, Inc. v. Verio, Inc.¹²³</td>
<td>Medium: limited to Web pages, etc.; some uncertainty about consent</td>
</tr>
<tr>
<td>CFAA</td>
<td>Unauthorized intrusion into computer systems</td>
<td>Register.com, Inc. v. Verio, Inc.</td>
<td>Medium: potentially strong, though intended to prevent hacking; mental state requirement</td>
</tr>
</tbody>
</table>

As Table 3 demonstrates, a legal infrastructure for the cyberproperty right exists, but its net effects are far from clear. In particular, note the relatively high degree of uncertainty surrounding 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 on which to begin the policy analysis.

¹²². Kelly v. Arriba Soft Corp., 280 F.3d 934 (9th Cir. 2002), withdrawn and superseded, 336 F.3d 811 (9th Cir. 2003).
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.

**TABLE 4. The software environment for cyberproperty**

<table>
<thead>
<tr>
<th>Technology</th>
<th>Complexity</th>
<th>Effectiveness</th>
<th>Flexibility</th>
<th>Regulatory Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>http_referer (Server-side)</td>
<td>High: requires CGI development/ software installation &amp; configuration on server</td>
<td>Low: obscuring referrer header avoids it</td>
<td>Low: considers only referring page</td>
<td>Low: depends on default implementation</td>
</tr>
<tr>
<td>http_referer (Javascript)</td>
<td>Low: simple one-line code in html document</td>
<td>Low: obscuring referrer header avoids it</td>
<td>Low: considers only referring page</td>
<td>Low: depends on default implementation</td>
</tr>
<tr>
<td>Cookie Redirection</td>
<td>Medium: requires either CGI scripting or complex javascript</td>
<td>Low: cookie rejection is typical</td>
<td>Medium: cookies offer flexibility in information, but this generally requires prior visits</td>
<td>Medium</td>
</tr>
</tbody>
</table>

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 important to note that Table 4 represents the best available information as of the Summer of 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 clear below, this inflexibility in the software-regulatory environment has important implications for the analysis here.

127. See, e.g., GARFINKEL, supra note 124, at 280–92.
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 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 law or software is not enough.

In fact, the complexity of the law-software interface is perhaps even greater than the brief overview above. 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 Web sites (that is, for example, links to www.law.upenn.edu) versus “deep linking” (that is, 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 error). 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 Web site owners at least some legal protection against unwanted access. Second, again as outlined above, there also exists a range of software-regulatory options that can also serve a protective function in at least some respects. Together, these two factors suggest that the basic regulatory framework noted in Part 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, in the overwhelming majority of cases owners of network resources choose 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 eighty-five percent of Web sites allow full access. A survey of the top twenty-five Web properties found that only one—Ticketmaster.com—appeared to restrict all Web linking whether legal or technological. 129 Among the group, approximately half of the sites used the robots exclusion standard (robots.txt) to restrict the use of Web robots at all—and none excluded them entirely. 130 On the other hand, there are unquestionably a large number of Web sites that are not publicly accessible and that use various technological means (such as passwords and access-restricting firewalls) 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 ninety percent of Web sites and Web site owners want to allow either full or severely limited access to their sites—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; for “no access” the


130. The Robots Exclusion Standard is a voluntary standard to control the behavior of automated Web robots (“bots” or “crawlers”), which are most typically used to index content for search engines. A Web site owner can place a simple text file (“robots.txt”) at the top level of the site; the file defines the scope of access for robots. See Web Robots Pages, supra note 126.
technology exists (see “Authentication” in Table 2 above) to effectively cordon off these sites. Thus, the argument goes, why impose the costs and complexity of a regulatory environment when perhaps ninety 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, in the realm of conditional access. For example, a Web site owner might want to implement a business model that requires site visitors to traverse certain Web pages, requires them to view certain advertising, or simply ensures 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 the site and when. In each of these cases, neither the full access nor the no access condition addresses the problem effectively.

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 this ten percent is most likely to represent innovation in business models (or models of presenting information) online. In an era where most innovative 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 in the future. And yet if there is one thing we do know about the future of cyberspace, it is that we likely have not 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 appear weak.\textsuperscript{131} Such litigation is not socially beneficial. For one thing, such efforts may succeed in ways that create unintended

\textsuperscript{131} This is a good explanation of \textit{Kelly v. Arriba Soft Corp.}, 280 F.3d 984 (9th Cir. 2002), \textit{withdrawn and superseded}, 336 F.3d 811 (9th Cir. 2003), where Kelly was dissatisfied with the state of protection for his business model in selling his photos through his Web site.
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 such efforts do not succeed, they will almost certainly increase the uncertainty and instability across the board.

A third important reason that cyberproperty should encompass more complex options is that, as David McGowan has explained, such protections are more likely to support an ecosystem of diverse online spaces.\textsuperscript{132} 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 for a flourishing of differentiated sites.\textsuperscript{133}

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

One such consideration is the importance of establishing a clear default rule. Here, the recognition that the vast majority of network resources are offered without access restriction 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 when 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.\textsuperscript{134} Indeed, irrespective of the ultimate quantum of protection in the cyberproperty regime, such a rule would clearly be an advantage over the present set of circumstances, in which 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 toward 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

\begin{itemize}
\item \textsuperscript{132} McGowan, \textit{supra} note 26, at 360–62.
\item \textsuperscript{133} \textit{id.}
\item \textsuperscript{134} Here, for example, a single line in a TOS agreement would not be sufficient. Far more direct forms of notice would be required.
\end{itemize}
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. 135 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). 136 Therefore, for the all-important default rule, the analysis suggests that legal code should establish the parameters and should perhaps directly regulate software code as part of the process for altering the default condition in favor of full access.

C. THE FLEXIBILITY IMPERATIVE

As suggested above, there is perhaps no more important consideration in the context of cyberspace than the necessity of maintaining and improving the environment for innovation, experimentation, and entrepreneurship. Indeed, this might be the hallmark of the Internet, and the World Wide Web in particular; the benefits received thus far from the inherent mutability of the Internet 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 4 amply demonstrates, many of the 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; while this may be better than no information at all, it is 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. Cookies require users to have prior history with the site,
however, 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 law or other legal definitions of harm, as suggested by Dan Burk,\textsuperscript{137} 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 e-mail servers, for example) has important public good effects by facilitating the rapid exchange of information and ideas, as well as allowing the rapid innovation and development cycles that are a hallmark of the online environment. One argument that has consistently been made against a cyberproperty right is that such a regulatory condition, by reducing Web linking, for example, would 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 IV.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 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 some insight 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 IV above, this criteria argues rather strongly for a predominantly legal solution, though perhaps with software-implemented transacting.

\textsuperscript{137} Burk, supra note 26, at 53. See infra note 143 and accompanying text.
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 and the discussion in Part III demonstrate, given the current state of technology, a predominantly legal framework seems far more likely to provide stability and clarity going forward.\textsuperscript{138}

Third, as noted in Part 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 strongly in favor of more law and less software in the regulatory condition.

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 Part III above, depending on 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. As noted in Part IV above, however, there are a variety of forms of legal-regulatory approaches available. An important element in any policy analysis is evaluating these as well.

The choice of legal rule in the cyberspace context contains two axes of inquiry.\textsuperscript{139} The first is the fairly traditional dichotomy between property

\textsuperscript{138} This argument assumes substantial clarification in the doctrinal framework for the cyberproperty right.

\textsuperscript{139} See supra Part IV.
rules and liability rules, with the general argument being that property rules are better when the costs of bargaining are relatively low. In the cyberproperty context, a property rule will establish the basic right of Web developers to determine access and presumes that contractual arrangements will define the details of such access. A liability rule, by contrast, defines much of the details of the arrangement, typically allowing use except when 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 or forms of linking that border on misappropriation.

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) to supporting software regulations (generally forbidding the obscuring of the http_referer header, for example), to supporting transactional mechanisms (requiring the use of software to provide notice or enable transactions, for example).

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. Bellia, McGowan, and Richard Epstein, for example, suggest that bargaining is possible in this context, and that the property rule dominates. Burk and Maureen 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 Internet, argue instead for a liability rule. A recent decision by the

---

140. See supra notes 79–86 and accompanying text.
141. See McGowan, supra note 26, at 375–76.
142. Perhaps knowingly triggering the Slashdot Effect. See Adler, supra note 81.
143. Such forms may include inline linking to others’ images as in Kelly v. Arriba Soft Corp., 280 F.3d 934 (9th Cir. 2002), withdrawn and superseded, 336 F.3d 811 (9th Cir. 2003), or the framing of content (displaying content from another site in a frame in a Web page so that it appears to be a part of the local site).
144. See Bellia, supra note 16; Epstein, supra note 26, at 84; McGowan, supra note 26, at 382–85.
145. See Burk, supra note 26; O’Rourke, Analogy, supra note 26.
Supreme Court of California comes down rather strongly in favor of liability rules (if any entitlement is indeed available).\footnote{See Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003).}

And yet, as the analytic framework of this Article has suggested, these now familiar arguments on both sides of the property rule versus liability rule debate 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 Part III above, outlined the general framework for evaluation here, and it is worth revisiting that table here.

\begin{table}
\centering
\caption{Features of property versus liability rules}
\begin{tabular}{|l|c|c|c|c|c|}
\hline
Rule-Form & Flexibility & Institutional Intervention & Response Time & Transaction Costs & Embedding Public Values \\
\hline
Property Rule & High & Low & High & High & Low \\
Liability Rule & Low & High & Low & Low & High \\
\hline
\end{tabular}
\end{table}

As was suggested above, the analytic approach is a multifactor 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. The following provides a brief overview of each factor in Table 2 in this specific context.

\textit{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, and how it is built, maintained, and accessed: sites are typically top-down and generally hierarchical; they collect related information and use pages to separate and hold content; they integrate text, images, and multimedia, link internal pages through the use of menus; and so on. Perhaps even more important, people typically conceive of Web site providers as allowing free access to all comers, with some relying on advertising revenue or an authentication backed subscription model in rare cases. But these current
conceptions of the “way the Web works” are just that: current conceptions. If the history of the World Wide Web teaches us anything, it is that its value lies in the huge array of experimental approaches it has fostered. Many of these experiments have failed spectacularly. Others have succeeded. And for some prominent players, the jury is still out.

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

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 have some level of familiarity with the thing that is to be regulated, 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; 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 seems highly advantageous. Thus, this factor seems to favor a property rule.

Transaction costs. One of the driving forces of innovation in this context is the relatively low cost involved in building, developing, and maintaining a Web site. In some ways, of course, this obscures the fact that a huge quantity of Web sites populating the Web means that great costs are likely to be incurred in building traffic. Thus, anything that would greatly

147. Web sites such as Pets.com and Webvan are good examples.
148. Examples include Yahoo!, eBay, and the Wall Street Journal Online.
149. One example is Amazon.com.
increase the costs of engaging in such development should be avoided. Indeed, concern about transaction costs is perhaps the most invoked argument against property-type rules in the cyberproperty context.  

While increased transaction costs are at least a viable concern, the choice of legal rule can address it. It might do so in at least two ways. First, the establishment of a strong default rule in favor of open access—that is, one that requires meaningful notice to vary the default condition—will, as suggested above, greatly reduce the quantity of necessary transactions. In other words, 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 rule 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 factor. 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 factor.

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. The second public value is related to free expression principles: the ability of Web developers to use Web technologies (linking and access, for example) as part of their expressive purpose. The third value is more closely related to competition issues: the concern that more variance in access requirements will allow some sites, particularly commercial sites, to limit competition by imposing access requirements.

There is little doubt that the Internet and widespread access to the Web greatly benefit the public. The question is how much this impacts a choice of rule analysis. For if the assumption noted above is correct—that

151. But see McGowan, supra note 26, at 376–78 (arguing that transaction costs will be low).
152. See Burk, supra note 26, at 47–48; Hunter, supra note 5; Lemley, supra note 118.
153. See Hunter, supra note 5, at 488–94 (discussing First Amendment jurisprudence, especially public forum doctrine, as applied to cyberspace).
perhaps eighty-five to ninety percent of Web developers 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 will not
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 should not have much impact on this eighty-five percent. This holds
ture if reasonable hurdles are established to change the default condition,
such as clear notice requirements or the use of technological means to
provide notice or facilitate transactions. And, as noted above, the effect on
the remaining ten to fifteen percent of 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 value of the Internet is clearly
important, it is far from clear how much its value should 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 rights holders to enforce their rights under neutral laws without
raising First Amendment objections.\footnote{155} In some cases, narrow exceptions
to property rules might be warranted.\footnote{156} 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 relate more to corporate behavior as measured by traditional
competition policy principles, rather than to the choice of legal rule-form
for a general cyberproperty entitlement.\footnote{157}

As a general matter, this prong seems to favor a liability rule, though
perhaps less strongly when compared with a property rule incorporating the

Rowan v. U.S. Post Office Dep’t, 397 U.S. 728, 737 (1970); Eldred v. Reno, 239 F.3d 372, 375–76
(D.C. Cir. 2001), amended by 534 U.S. 1160 (2002); Epstein, supra note 26, at 85–87; McGowan,
supra note 26, at 365–66.}

\footnote{156. See, e.g., 17 U.S.C. § 107 (2000) (detailing the fair use defense to unauthorized use of a
copyrighted work).}

\footnote{157. Portions of the Sherman Antitrust Act of 1890 may be illustrative here. See 15 U.S.C. §§ 1–2
(2000). See also McGowan, supra note 26, at 383 (doubting the possibility of widespread
anticompetitive behavior in this context).}
default condition noted above, and perhaps 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 far from over. The normative decision must be considered in light of what Part IV 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

Part IV demonstrated that the choice of legal rule-forms cannot occur in a vacuum. It must incorporate an understanding of the rule’s instrumental performance, and its ability to affect the law-software interface; it must also 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 Part 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 does not maximize) software regulation. Second, regardless of whether one believes the potentially negative effects of overuse of software regulation, Part 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.158

In the cyberproperty context, there is little to suggest that the general approach outlined in Part IV 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.159 This principle suggests, therefore, that the

158. See supra Part II.
159. See supra notes 99–113 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
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 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:

Property rule: a rule that generally offers clear entitlements to
injunctive remedies to Web site owners for unauthorized access; and

Default condition: a default presumption in favor of open access, with
nontrivial requirements of notice to vary this default; and

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
Part V.A.

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—to change the default
condition. It is also related to the result in *eBay v. Bidder’s Edge, Inc.*,
which fundamentally upheld the access conditions established by eBay’s
robots.txt file.\(^{160}\)

This part 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

\(^{160}\) See *eBay, Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000). Note also that
McGowan and Epstein reach a generally similar result, albeit via a different analytic path. See Epstein,
approach, a richer, more nuanced analysis is available. Consistent with these general observations, this part suggests that in the cyberproperty context, an overreliance 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, is necessarily conditional along a variety of dimensions. Consistent with a theme of this Article, as technological circumstances change, the analysis will also change. Furthermore, notwithstanding its multifaceted nature, the process followed here requires a number of balancing decisions—at least some of which could yield a different result. Despite these issues, however, the case of cyberproperty illuminates both the challenges in and benefits of understanding the law-software interface.

VI. 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. Less law does not necessarily mean more freedom.

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

While this framework is highly dependent on 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, 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 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 telecommunications and media creation and distribution, the relevance of analytic processes that address both law and software will only increase. Unquestionably, software regulation is here to stay. The real questions are whether our policy approaches can meaningfully account for this trend, and whether the case against software will be fully understood.

VII. APPENDIX

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 (nondefault) 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:161

<table>
<thead>
<tr>
<th>Metag</th>
<th>Description of Use</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keywords</td>
<td>Lists subjects of the Web page, intended to assist Web searching and indexing</td>
<td><code>&lt;meta name=&quot;keywords&quot; content=&quot;[. . .keywords. . .]&quot;&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>Describes the content of the Web page, intended to assist in Web searching</td>
<td><code>&lt;meta name=&quot;description&quot; content=&quot;[. . .description. . .]&quot;&gt;</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Metatag</th>
<th>Description of Use</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>PICS-Label162</td>
<td>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 (for example, “sexuality” or “violence”)</td>
<td><code>&lt;meta name=&quot;pics-label&quot; content=&quot;[codes indicating the level of certain types of content]&quot;/&gt;</code></td>
</tr>
<tr>
<td>Content-type</td>
<td>Tells the Web browser what specification the page is encoded for</td>
<td><code>&lt;meta name=&quot;content-type&quot; content=&quot;[codes indicating the level of certain types of content]&quot;/&gt;</code></td>
</tr>
<tr>
<td>Expires</td>
<td>Used for caching purposes; an “expired” page is not served by the caching mechanism</td>
<td><code>&lt;meta name=&quot;expires&quot; content=&quot;[date and time]&quot;/&gt;</code></td>
</tr>
<tr>
<td>Author</td>
<td>Tags for the author of the content</td>
<td><code>&lt;meta name=&quot;author&quot; content=&quot;[author name]&quot;/&gt;</code></td>
</tr>
<tr>
<td>Generator</td>
<td>Tags for the software used to create the content</td>
<td><code>&lt;meta name=&quot;author&quot; content=&quot;[software name]&quot;/&gt;</code></td>
</tr>
</tbody>
</table>

Metadata that described access or linking policies (or both) would then be available for a variety of automated or machine-assisted tasks. For example, Web browsers could be configured to load only those pages with certain metadata or with open access, or information about linking rights could be utilized by Web development software packages or link checkers to allow automated clearance of linked-to sites.163

More sophisticated technologies could use metadata information to perform actual transactions. For example, perhaps a $0.0001 charge per page view of the Wall Street Journal Online could be deducted from one’s

162. See, e.g., World Wide Web Consortium, supra note 95.
163. Link checker software is commonly used to verify that all links (both internal and external) on a page are “live,” or functioning. It would be relatively easy to incorporate actions or reporting of such programs based on the metadata encountered.
bank account, or Web development software could report the conditions on which linking is authorized—“only link to Home,” “only send 1000 hits per day,” or “no traffic on Tuesdays”—which could of course be incorporated into modern Web sites.  

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.

164. See generally PHILLIP GREENSPUN, DATABASE BACKED WEB SITES: THE THINKING PERSON’S GUIDE TO WEB PUBLISHING (1997).