2005

Reconsidering the DMCA

R. Polk Wagner
University of Pennsylvania Carey Law School

RECONSIDERING THE DMCA

*R. Polk Wagner**

TABLE OF CONTENTS

* Professor, University of Pennsylvania Law School. I am indebted to the participants of the 2005 IPIL/Houston Santa Fe Conference: *Transactions, Information and Emerging Law* for helpful comments on earlier drafts. Kevin Goldman, Danielle Rosenthal, Al Dong, and Ed Greenlee provided excellent research support.

I. INTRODUCTION

The Digital Millennium Copyright Act (DMCA)[1] is a law that nearly all legal scholars love to hate. As an industry-backed response to the radical advances in digital technology and network communications, the relevant terms of the law seem broadly consistent with a view that the DMCA was intended to protect the then-existing distribution models for copyrighted content during an era of great transition.[2] Put more directly, Hollywood called for action, and Congress (and the President) responded.[3] Given this backdrop, the dominant understanding among observers and commentators is that the DMCA altered the inherent balance in copyright law between the copyright owners (e.g., Hollywood) and the public (e.g., users or consumers) in favor of the copyright owners.[4]

This Essay suggests that a reconceptualization of the DMCA may be in order. Rather than looking at the anticircumvention provisions of the DMCA as moving the fulcrum along the copyright scale, I urge that we consider anticircumvention as a law addressing the regulatory effects of technology.[5] In the anticircumvention provisions, Congress did not in fact alter the balance between copyright owners and the public—very few users of copyrighted goods are implicated by these rules.[6]

---

1. Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

2. *See* Joseph P. Liu, *The DMCA and the Regulation of Scientific Research*, 18 BERKELEY TECH. L.J. 501, 502 (2003) (noting that supporters of the DMCA find the provision "necessary to prevent unauthorized copying of copyrighted works in the digital environment").

3. *See, e.g.*, John Schwartz, *The Net Impact of the New Copyright Bill*, WASH. POST, May 18, 1998, Washington Business, at 27 (stating that the main supporters of the DMCA are influential holders of copyrights in the entertainment industry).

4. The DMCA is heavily discussed in legal literature. Indeed, a recent Westlaw search (in the "JLR" database) identified at least 53 articles using the term "DMCA" in the title, and more than 1480 containing the term. Notwithstanding the volume, this Author is aware of only two prominent defenses of the anticircumvention provisions of the DMCA in print. *See* Jane C. Ginsburg, *Copyright and Control over New Technologies of Dissemination*, 101 COLUM. L. REV. 1613, 1636 (2001) (arguing in favor of anticircumvention provisions); Orin S. Kerr, *A Lukewarm Defense of the Digital Millennium Copyright Act*, *in* COPY FIGHTS: THE FUTURE OF INTELLECTUAL PROPERTY IN THE INFORMATION AGE 163, 163–70 (Adam Thierer & Wayne Crews eds., 2002).

5. There are multiple provisions of the DMCA. This Essay is concerned only with what are generally described as the "anticircumvention" and "copyright information integrity" provisions. *See* 17 U.S.C. §§ 1201–1202 (2000). For simplicity, references to the DMCA or to "anticircumvention" should be understood to mean these sections of Title 17.

6. The DMCA's anticircumvention rules broadly target the development, use, and distribution of circumvention technologies. *See infra* Part III. A user who makes an unauthorized copy of a copyrighted work (irrespective of whether that work was made

Instead, Congress attempted to alter the balance between law and software to respond to changes in the enforcement environment by shifting the regulatory equilibrium back towards the law. Therefore, these statutory provisions are perhaps the first major example of an emerging feature of the modern regulatory environment: the direct manipulation of regulatory effects on software code via the law—or what I describe as "legal preemption."[7]

Legal preemption is a creature of the digital, networked age—an era when goods, services, contracts, transactional communications, and enforcement mechanisms are all just collections of bits streaming through the global data networks. In 2005 it is a cliché to observe that software code has important regulatory effects in this environment—as Lessig put so adroitly, "code is law."[8]

It is well understood that the line between products and the contracts that govern them, if there ever was a meaningful line, is growing increasingly indistinct. It is further understood that underlying legal concepts, such as property-like rights granted by copyright law, are a foundation (albeit an important one) for the product-contract transactions they support. But recognition does not necessarily lead to real understanding. What is often lost in the code-is-law perspective is the broader view of the modern regulatory environment as equilibrium between the software and legal "codes."[9] Under this view, law and technology are linked, and it is the interaction between the two that determines the regulatory effects.[10]

Recasting legal code and software code as complementary, rather than as pure substitutes, leads to a number of important observations. First, all discussion of regulation in the transaction of digital goods must consider both legal and technological dimensions of the enforcement equation; looking at law or software in isolation simply misses the point.[11] Second, the development of regulatory policy in this new digital era offers

---

available via the circumvention of protection technology) is not legally affected by the DMCA.

7. *See* discussion *infra* Part II.D.

8. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999) (explaining that "the software and hardware that make cyberspace what it is *regulate* cyberspace as it is").

9. *See* R. Polk Wagner, *On Software Regulation*, 78 S. CAL. L. REV. 457, 465–77 (2005).

10. *Id.* at 468–70.

11. *Id.* at 465–74.

both perils and promise.[12] On the one hand, traditional lawmakers control less of the regulatory framework than ever before and lack important information about the true effects of any legal intervention.[13] On the other hand, legal code remains enormously powerful, and the legislative and judicial options have just expanded.[14]

It is on this last point that this Essay will focus. When law and software together create the net regulatory environment, policymakers will necessarily affect more than the simple allocation of rights among competing parties (here, for example, among content owners and the consuming public); they will also affect the location of the law-software interface.[15] In other words, modern regulatory policy implicates both the substance and the mechanism of regulation, and establishes the mixture between legal code and software code.[16] Thus enters the era of legal preemption: the attempt to use legal mechanisms to directly alter the law-software equilibrium. The DMCA's anticircumvention provisions, by squarely addressing the technological aspects of the regulatory environment for copyrighted goods,[17] represent a first look at this brave new world of legal preemption.

This Essay proceeds as follows. Part II lays the foundation by drawing on earlier related work to develop an analytic outline for the digital regulatory environment. Rejecting the simplistic mantra of code-is-law, this new analytic outline emphasizes the dynamic and often unpredictable interaction between legal code and software code, as well as the important implications of different code mixtures. The analytic outline recognizes that legal code and software code regulate in very different ways, with different strengths, weaknesses, costs, and benefits. Indeed, there are good reasons to believe that software regulation can have undesirable effects, that it will substitute speed and effectiveness for flexibility and critical enforcement "safety valves." A policy mandate for more law and less software is perhaps best met via the use of legal preemption or the direct alteration of the law-software regulatory interface.

---

12. *Id.* at 474–77.

13. *Id.*

14. *See* Michael A. Carrier, *Cabining Intellectual Property Through a Property Paradigm*, 54 DUKE L.J. 1, 8–17 (2004) (examining the expansion of copyright protections).

15. Wagner, *supra* note 9, at 474; elaborated upon *infra* Part II.

16. Wagner, *supra* note 9, at 470–74; elaborated upon *infra* Part II.C.

17. *See* 17 U.S.C. § 1201 (2000).

Part III picks up this thread and considers the DMCA's anticircumvention provisions as a form of legal preemption. That is, given the context established in Part II, Congress's choice of statutory provisions is revealing: Rather than addressing the users of infringing goods, Congress clearly sought to affect the way that technology would be deployed. Importantly, the anticircumvention provisions have multifaceted effects on software regulation. In the near term, the law seeks to alter the current law-software mixture: simultaneously encouraging some forms of software code while banning others. The longer-term effects are perhaps even more significant: the DMCA provisions seem reasonably likely to reduce incentives for faster development of technologies that would further alter the equilibrium between law and software. That the DMCA might, contrary to the conventional wisdom, actually limit the development and deployment of "digital rights management" (DRM) in the field of copyrighted goods could be its most surprising, and important, regulatory legacy. Part IV concludes.

II. THE DIGITAL REGULATORY ENVIRONMENT[18]

This Part outlines a basic analytic framework for thinking about the relationship between the two major regulatory modes of the digital regulatory environment, law and software.[19] The core observation is that the law-software relationship is primarily complementary—it 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. Conceptually, the idea is to think in terms of equilibrium, the natural resting point on the law-software interface.

The analytic framework developed and explored here is based on the following premises:

(a) Both legal code and software code have regulatory effects;

---

18. This Part is based on a far more detailed treatment of this issue in an earlier work. *See* Wagner, *supra* note 9.

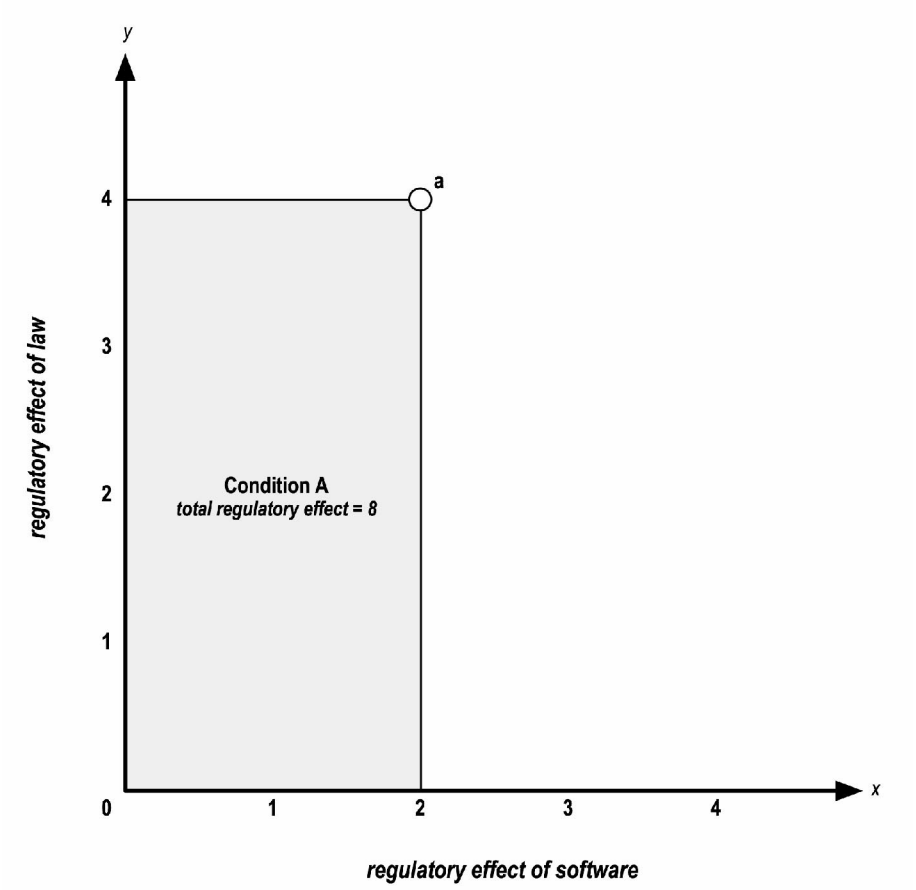
19. As Lessig has aptly noted, social norms and the marketplace will have important regulatory effects in cyberspace, as they do in realspace. Lawrence Lessig, Commentary, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 507–10 (1999). For simplicity, and because the most interesting 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.

(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.

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

Figure 1. The Law-Software Interface



Here, the axes represent the effects (or impact) of the two regulatory modes, law (y-axis) and software (x-axis). 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 x 4 = 8.

In the digital information goods 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 primarily by the protections and limitations of Title 17 of the U.S. Code.[20] The technological effects include both the availability of protection-enhancing software, such as DRM, as well as the existence of what Tim Wu describes as antiregulatory code—software that undermines the appropriability of the work.[21] What is important for establishing the equilibrium, and thus total appropriation, are the net effects of each regulatory system, law and software.

A. Equilibrium at the Law-Software Interface

Having established a basic understanding of the law-software equilibrium through Figure 1, it becomes crucial to understand the response mechanisms that produce this condition. One important point is that the responses can be expected to flow in both directions: Legal conditions will provoke a technological response, and technological circumstances can prompt legal changes. In the digital environment, 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.[22] 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). In the copyright context, evaluating this net legal impact presents content owners with a choice concerning whether to

---

20. *See* 17 U.S.C. §§ 101–1332.

21. 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. Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 726–45 (2003). Note that the impact of both law and software must be considered on a net basis. Just as software in the digital-goods context has both pro-protection and antiprotection effects, the Copyright Act provides both legal protections and legal limitations. *Compare* 17 U.S.C. § 106 (detailing a copyright owner's exclusive rights in a copyrighted work), *with* 17 U.S.C. § 107 (codifying the "fair use" defense to unauthorized use of a copyrighted work).

22. It also represents average behavior. Obviously, in the absence of explicit restrictions otherwise, 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.

deploy software-based regulatory mechanisms. For example, content owners could implement a strong regime of DRM, seeking to prevent unauthorized access to the work via technology. The use of this technique will increase the level of protection, though it obviously comes with a series of related costs, both monetary and otherwise. Ultimately, of course, 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.[23]

B. Dynamic Effects

Fleshing out this basic framework requires a few more details. Perhaps the most important and most straightforward of these observations is that the law-software interface is profoundly dynamic.[24] That conditions change, of course, is unremarkable. What makes the dynamic effects of the modern 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.[25] From a policy perspective, this observation is crucially important: It means that policy adjustments in the digital context cannot merely be contemplated as one-dimensional changes (or paradigmatically to legal scholars, as changes in the legal environment). 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 determines the overall regulatory environment.

---

23. Note also that the response effects do not flow in only one direction. Technological circumstances can drive legal changes.

24. 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.

25. Obviously, there are quite likely to be short-term effects where responses to change 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. The Interplay Between Regulatory Effects

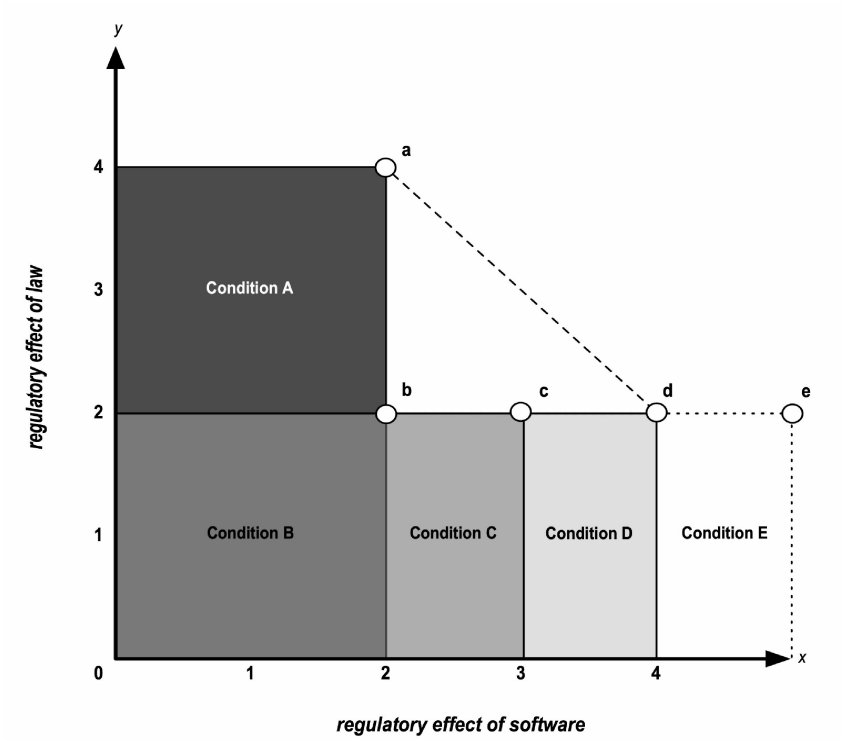


Figure 2 generally describes a change in legal regulatory effects (a decrease from 4 to 2, for example, when the law reduces a class of ownership rights), and explores the implications of various technological responses. Points *b*, *c*, *d*, and *e* describe a range of possible software responses, each 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 for example, it may be too inflexible to be useful.[26] In this case, total regulatory effect reduces from 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 or regulated good in Condition *B*; for example, if the regulatory environment for music or movies changed, one would expect a change in output. This could be

26. A bit of foreshadowing: Another possibility for Condition *B*, which I discuss more fully in Part II.D below, is that the legal regulation directly affects the quantity or nature of the software regulation, which I describe as legal preemption.

either a positive or negative change, depending 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 at least marginally in response to the decreasing legal regulatory effects. For example, the expansion of "fair use" exceptions to copyright infringement might yield an increased reliance on DRM-based solutions. This increase in software effects in Condition *C*, however, does not make up for the reduced legal effects, and the overall regulatory effects drop to 6 (3 x 2). As above, one should expect a change in output.

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 roughly fungible, at least from a net regulatory effects perspective.[27] 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.[28]

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 new regulatory context. 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. The intertwined relationship of law and software demands careful consideration of each. Code is not equivalent to law, a point that matters crucially in the modern legal-policy environment.

---

27. As discussed in some additional detail below and elsewhere, they are clearly not truly fungible even in this case. *See, e.g.*, Wagner, *supra* note 9.

28. An example might be "unbreakable" digital rights management (DRM) systems, or even copy-protected CDs that work reliably. Note that Condition *E* could also occur where cost-effective software responses are profoundly inflexible, essentially forcing deployment of more effective protections.

C. A Few Implications of Software Regulation

Understanding the basic framework developed above leads naturally to at least two important observations. The first is dynamism: 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. Further, because of the nature of technological change, even stable law-software equilibria are unlikely to remain so permanently.

The second observation, and the one central to this Essay, is that policy development in this context must consider both the desired net regulatory effects—for example, how much real protection to offer copyright owners—as well as the appropriate mechanism—the mixture of law and software. That is, law and software both regulate, but they are far from the same: they regulate in very different ways, are controlled differently (if at all) by traditional governmental authorities, and have quite different effects. Regulation in the digital era has an additional dimension, and the location of the law-software equilibrium may well be as important as the overall regulatory effect.

Indeed, as I have argued at length elsewhere, there is good reason to conclude that the overreliance on software code as a regulatory mechanism is not socially beneficial. The basic features of software code include:

- *Preprogramming.* 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.

- *A 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 significantly constrained by the creativity of the programmer, the complexity or sophistication of the software itself, or the environment in which it operates.

- *Self-containment.* The point here is obvious: Software-implemented regulations are free-standing mechanisms and do not generally require recourse to other institutional players for enforcement and rule determinations.[29] This

29. 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

> 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.
>
> • *Marginal costlessness.* Software regulatory operations are generally unaffected by the quantity of use.

Of course, 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. And yet these same features also have serious negative implications, including the lack of regulatory "safety valves," the elimination of marginal enforcement costs, and the potentially troubling public effects of software scalability.

1. Software-Based Regulation Lacks 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 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), and even issues of 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 appears to be purely private dealings will have substantially less impact where software is concerned.

2. Software Regulation Can Eliminate Marginal Enforcement Costs. It is axiomatic that the enforcement of legal rights will not occur where the enforcement costs outweigh the expected gains.[30] While enforcement costs are often viewed as a

---

mechanisms inherently combine information collection, rule analysis, and enforcement.

30. *See, e.g.*, R. H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 15–16 (1960)

social drag, their function of allowing for some low-level violations of rights can be in many cases beneficial; hence, the concept of "efficient breach" in contract law. This effect of enforcement costs is especially well understood in the area of intellectual property, where allowing the broadest possible dissemination of intellectual creations—consistent with maintaining appropriate development incentives—is a core value.[31]

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 that the effects noted above will not be realized.

3. Software Regulation May Scale Poorly. While, as a general matter, software scales well—its behavioral features remain unchanged as the quantity of activity increases—the scaling features of software may have potentially troubling public effects. For one thing, software regulation is likely to become increasingly vulnerable to countermeasures as the scale of its use increases;[32] 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.[33] Further, software regulation is unlikely to fail gracefully. Once bugs or countermeasures are discovered, the effectiveness of the particular regulatory mechanism is

---

(asserting that the "rearrangement of rights will only be undertaken when the increase in the value of production consequent upon the rearrangement is greater than the costs which would be involved in bringing it about").

31. *See* R. Polk Wagner, *Information Wants to Be Free: Intellectual Property and the Mythologies of Control*, 103 COLUM. L. REV. 995, 1001–02 (2003) (noting the tension between an incentive to produce and the desire to promote creativity and invention).

32. This situation is exacerbated by an institutional tendency to underreport potential defects at the performance testing stage prior to release. *See, e.g.*, H. Jeff Smith & Mark Keil, *The Reluctance to Report Bad News on Troubled Software Projects: A Theoretical Model*, 13 INFO. SYS. J. 69, 70 (2003) (describing how software developers and project managers are often unwilling to report the actual status of a "troubled project"); Lisa Liberty Becker, *Telling the Truth Can Be Hazardous to Your Job*, BOSTON GLOBE, Apr. 6, 2003, at G9 (observing the tendency to dismiss or minimize bad news in the quality assurance context). *See generally* RTI, THE ECONOMIC IMPACTS OF INADEQUATE INFRASTRUCTURE FOR SOFTWARE TESTING (2002) (studying the impact of inadequate software testing on the economy).

33. *See, e.g.*, Christopher Jones, *Internet Hacking for Dummies*, WIRED NEWS, Feb. 20, 1998, http://www.wired.com/news/technology/0,1282,10459,00.html. Eric Raymond famously made a similar point in the context of the open source movement, noting that "'[g]iven enough eyeballs, all bugs are shallow.'" ERIC S. RAYMOND, THE CATHEDRAL AND THE BAZAAR: MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY 41 (1999); *see also* Yochai Benkler, *Coase's Penguin, or, Linux and* The Nature of the Firm, 112 YALE L.J. 369, 434–36 (2002).

substantially diminished.[34] 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.

Combining the law-software framework with a recognition that high levels of software regulation could be unfavorable implies strongly that one goal (or at least consideration) of regulation in the digital environment should be to limit (or at least control) the quantity of software-based regulation.[35]

D. Software Regulation and the Choice of Legal Rules: Legal Preemption

In other related work, I have noted that where a regulatory objective is to limit the quantity of software-based enforcement in the overall regulatory environment, the use of property rules (as opposed to liability rules) is likely to be (at least weakly) favored. The flexibility, power, and scale of property rules enable participants in the marketplace to tailor a legal regime to meet rapidly changing circumstances.[36] This Essay seeks to explore another form of legal rule, one that is neither property nor liability but instead directly controls the law-software equilibrium. I call this type of rule legal preemption.[37]

Analytically, legal preemption is relatively straightforward: the use of the power of law to limit (or remove) the effect of software regulation. Obviously, this technique can take several forms, ranging from an outright ban on certain technologies,[38] to

---

34. *See* Dan Verton, *Tech Consortium Created to Improve Software Reliability*, COMPUTERWORLD, May 20, 2002, at 12 (noting that unreliable software costs companies over $175 billion per year to repair); *see also Building a Better Bug-Trap*, ECONOMIST, June 21, 2003, Technology Quarterly, at 15. *See generally* RTI, *supra* note 32 (discussing the effect that low-quality software has on the market, and the need for a software testing infrastructure that prevents the release of such software). Additionally, efforts to repair vulnerable or defective software systems are typically problematic. *See* George V. Hulme, *Quality First: Companies Pay Up to Plug Holes*, INFORMATIONWEEK, May 20, 2002, at 38 (observing that hackers outpace the repair efforts of security administrators); Douglas Schweitzer, *Emerging Technology: Patch Management, Patch Me If You Can!*, NETWORK MAG., Aug. 2003, at 40 (stating 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).

35. Complete elimination of software regulation in the modern regulatory environment is impractical.

36. *See* Wagner, *supra* note 9, at 491.

37. *See id.* at 484–88 (discussing legal preemption in the cyberlaw context, and its role as a form of legal regulation).

38. An example of this is the Audio Home Recording Act (AHRA), 17 U.S.C. § 1002(a) (2000), which defines the range of permissible operations for "digital audio recording device[s]" that fall within the scope of the Act.

enforced standardization,[39] to manipulating incentives, to developing and deploying either desired or undesired forms of software regulation. The different forms of legal preemption may be used individually or as a mixture. (As discussed below, the DMCA's anticircumvention provisions are an example of multiple forms of legal preemption in action.)

It should also be noted that legal preemption is not entirely a creature of the Internet: Regulators in many contexts have attempted to use the direct regulation of technology to affect the overall regulatory-marketplace environment. An outright ban on theft-enabling technologies, such as cable descramblers, is an extreme example.[40] A somewhat more subtle example is the use of prescribed efficiency and safety standards to regulate the automobile market.[41] The point here is that, in an era in which traditional legal leverage is waning, and more "technological" regulatory opportunities are emerging, we are likely to see an increase in the use of legal preemption in the modern online environment.

From a regulatory toolbox perspective, the advantages of legal preemption are clear.[42] Most importantly, it provides a vehicle by which the law can directly affect the law-software equilibrium point.[43] Instead of attempting to predict the technological response to a legal change,[44] legal preemption has a far more predictable effect. Additionally, a legal preemption strategy—by seeking to "freeze" (or at least slow) the relevant software-regulatory developments—can add stability and certainty to an area of regulation. Finally, because legal preemption does not directly affect the substantive level of regulation (though, as noted above, it can clearly have an important effect) this approach may bring political advantages.

But there are also potential concerns with a legal preemption approach. One potential problem is with feasibility. While in theory it should be possible to directly address virtually

---

39. For example, the Federal Communications Commission (FCC) mandates various technical standards relating to digital broadcast television. *See* Edmund L. Andrews & Joel Brinkley, *The Fight for Digital TV's Future*, N.Y. TIMES, Jan. 22, 1995, at F1.

40. *See* 47 U.S.C. § 553(a) (2000).

41. *See* 49 U.S.C. § 32902 (2000) (establishing average fuel economy standards); § 30111 (discussing safety standards for motor vehicles).

42. *See* Wagner, *supra* note 9, at 492–93 ("[T]he goal of a rule of legal preemption is fixing . . . the corresponding regulatory effects of software.").

43. *Id.* at 485–86 ("[T]hese supportive regulations serve to stabilize the law-software equilibrium point by reducing the incidence of at least some forms of anti-regulatory code.").

44. *See supra* Part II.B.

any software regulation with a legal rule, the rapid pace of development and inherent uncertainty involved in modern technology at least raise questions about the practicability of this approach. An additional problem with this approach is the fact that the pace of legal change (whether by legislation or judicial decision) typically moves comparatively slowly and often involves institutional actors whose competence in modern technologies is, to say the least, not assured.[45]

A second potential problem is that the costs of error in legal preemption might be unusually high. The direct manipulation of technology could serve to "lock-in" an unfortunate set of circumstances, could forestall developments that might lead to more socially beneficial arrangements or even have more general unintended spillover effects on technological change. For example, a legal rule barring peer-to-peer technologies can be predicted to: (1) favor the current incumbent distributors in the digital media business, together with their (arguably inappropriate) business models; (2) substantially slow the current transition in digital media distribution models, delaying more efficient forms of this business; and (3) dissuade some investments into peer-to-peer and related technologies for fear of legal liability in the future.

Despite these potential downsides, which are significant and highly plausible, there is good reason to expect that the policymakers of the future will turn to legal preemption techniques with increasing enthusiasm. First, as noted above, legal preemption is perhaps the most obvious way to solve the major regulatory challenge of our time: the shift in power from legal code to software code. Second, for lawmakers in an era where traditional, sovereign-state-based government is becoming increasingly marginalized, legal preemption is an attractive way to reposition themselves at the forefront of regulatory activity.

III. RECASTING THE DMCA

This Part argues that the anticircumvention provisions of the DMCA are a prescient example of legal preemption—a harbinger of what is likely to be an important mode of regulation in the digital era. By directly addressing the regulatory technology in digital media markets, the DMCA is an effort by

45. *See* Matthew Fagin et al., *Beyond Napster, Using Antitrust Law to Advance and Enhance Online Music Distribution*, 8 B.U. J. SCI. & TECH. L. 451, 573 (2002) (preferring specialized agencies to generalist courts that may lack expertise necessary to understand complex economic and technological issues surrounding digital distribution of music).

lawmakers to exert control over the law-software interface in one of the most rapidly-changing areas of the economy.

The DMCA is a particularly important example of legal preemption not only because of its context. The anticircumvention rules have features which make them an interesting case study into this emerging regulatory technique. For example, as discussed below, the DMCA both suppresses technology (anticircumvention technology) as well as encourages technology (access control technology, or DRM): an effort to shift the law-software interface using both the carrot and the stick. Further, and perhaps most importantly, the DMCA is likely to limit the incentives for an "arms race" in DRM (and anti-DRM) technologies, thus effectively restraining the development and deployment of DRM. Indeed, for those who have concerns about the social benefits of DRM and related software-based regulatory technologies, the anticircumvention provisions of the DMCA might be a positive step rather than a negative; it may well be that the DMCA should be understood as a law that moderated the growth of DRM in a critical area.

This Part continues as follows. First, the case is briefly made as to why the anticircumvention provisions are best understood as legal preemption. Second, the DMCA's dual approach—both encouraging and suppressing software regulation—is discussed. Finally, the way that the DMCA in effect limits the growth of DRM is outlined.

A. Anticircumvention as Legal Preemption

The most relevant of the DMCA's anticircumvention provisions are codified at 17 U.S.C. § 1201, and read in part:

> (a) Violations Regarding Circumvention of Technological Measures.—
>
> > (1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. . . .
> >
> > . . . .
> >
> > (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
> >
> > (A) is primarily designed or produced for the purpose of circumventing . . . ;

> (B) has only limited commercially significant purpose or use other than to circumvent . . . ; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing . . . .
>
> . . . .
>
> (b) Additional Violations.—
>
> (1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing protection . . . ;
>
> (B) has only limited commercially significant purpose or use other than to circumvent protection . . . ; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection . . . .[46]

Broadly, the anticircumvention provisions prohibit the use, development, or distribution of technologies which are designed to "circumvent" (e.g., hack, crack, or break) access control systems (or DRM). There are a couple of important points here.

First, the anticircumvention provisions squarely address technology, not copyright.[47] That is, the terms of the rules are related to copyright only in the sense that the "circumvention" that is prohibited is one which voids an access control on a copyrighted work. Otherwise, copyright laws—the rights, limitations, and remedies afforded owners and the public—are not implicated.

Second, the anticircumvention rules do not generally affect the users of copyrighted work. By their nature, these technologies are likely to be rather esoteric, the province of sophisticated computer users.[48] Thus, the quantity of users of a

---

46. 17 U.S.C. § 1201(a)–(b) (2000).

47. *See* JAY DRATLER, JR., CYBERLAW: INTELLECTUAL PROPERTY IN THE DIGITAL MILLENNIUM § 2.07[1] (2005) ("Section 1201 . . . is not part of copyright law and was never intended to be so. . . . Its focus is . . . entirely on *access* to copyrighted works. . . . Copyright law has never, and does not now, prohibit unauthorized *access* to copyright works.").

48. *See, e.g.*, Stephen M. Kramarsky, *Copyright Enforcement in the Internet Age: The Law and Technology of Digital Rights Management*, 11 DEPAUL-LCA J. ART & ENT. L. & POL'Y 1, 10 (2001) ("[T]he new anti-circumvention laws prevent *sophisticated users*

copyrighted work that are implicated by the anticircumvention provisions will be small. Also, note that the relevant provisions of the DMCA do not prohibit any particular use of the copyrighted work, irrespective of whether DRM was circumvented. Thus, the overwhelming majority of users will be in the same position after the DMCA as before it.

Therefore, because these provisions of the DMCA (1) directly address technologies, their creation, and their distribution; (2) do not directly alter the underlying copyright balance between creators and users (e.g., the substance of the copyright law is not changed); and (3) do not implicate the vast majority of the users of a copyright work (even one which is protected by DRM), the DMCA is not really a law about copyright. It is instead a law about technology. More specifically, it is a law that seeks to define the relationship between the legal code and software code. The anticircumvention rules are a clear example of legal preemption—the use of the law to (try to) control the code.

B. Encouragement and Suppression of Software Regulation

Even beyond the fact of legal preemption, the DMCA's basic structure has an interesting feature: it simultaneously suppresses and encourages technology. That is, on the one hand it encourages the deployment of "access control" technologies on copyrighted works—without them, any extra rights or remedies from the anticircumvention provisions are unavailable. On the other hand, it prohibits the use, development, or distribution of "circumvention" technologies.[49] Thus, the DMCA can be understood as trying to shift the law-software equilibrium for copyrighted goods generally in favor of software regulation, though it does so in two ways: by increasing the amount of software code that is deployed and by prohibiting antiregulatory code. The expectation is plainly that the net result here will be an increase in software regulation—and in that sense, at least a potential increase in overall regulatory effect because the DMCA does not change the underlying substantive legal rights.

C. The Plot Twist: How the DMCA Might Limit DRM

From the above discussion, it seems abundantly clear that the anticircumvention provisions of the DMCA are a form of legal preemption—their goal is to increase the net effects of software regulation in the digital copyright regime. Thus far, the proffered

---

from bypassing the technology." (emphasis added)).

49. *See* 17 U.S.C. § 1201(a).

conceptualization of the DMCA has yielded new insights, but the conventional wisdom about its origins and goals (as an additional grant of protection to the media-content creation industry) has been largely upheld.[50]

And yet there is an important additional feature to these legal rules, a feature that may, in fact, change the way we think about the DMCA in a more fundamental way. In its structure, the anticircumvention rules may effectively limit the incentives to create ever-stronger DRM solutions. It does so in the way that DRM technologies are described in § 1201 as a "technological measure that effectively controls access."[51] The key phrase here is "effectively controls," which has been interpreted (correctly, given the legislative context) to establish a low bar for the "strength" of the DRM, or its resistance to being hacked.[52] This low bar is, I think, crucial to this aspect of the DMCA. By setting a low bar for the effectiveness of DRM technologies, Congress provides incentives to content owners to meet that low bar—at which point these additional incentives disappear. In other words, the DMCA requires only somewhat weak DRM systems to qualify for the protection against anticircumvention technologies; once that threshold is reached, the law provides no additional rewards for further sophistication. Of course, there may well be other, nonlegal, incentives that point towards stronger DRM, such as a response to more effective attacks or the desire to structure transactions in a different way. But the point here is that when you put together these two aspects of the DMCA's anticircumvention provisions—(1) the low bar required for a content owner to receive protection and (2) the direct suppression of anticircumvention technologies—the net effect of the law will likely do three things. First, it will encourage the development and deployment of (relatively weak) DRM. Second, it will at least moderate the incentives to engage in an "arms race" for stronger DRM. Third, it will significantly suppress the incentives to use, develop, and distribute anticircumvention technologies of any kind.

---

50. *See* Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 422–25 (1999) (noting that the anticircumvention provisions were a response to lobbying by the media industry).

51. 17 U.S.C. § 1201(a).

52. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 441–42 (2d Cir. 2001) (noting that merely because a technological measure "was so easily penetrated" does not indicate that it does not "'effectively control[] access'" within the meaning of § 1201(a)(2)(A) (citing Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000))).

This suggests that one real possibility for the long-term effects of the DMCA is that it will slow or stabilize the development of DRM technologies in the digital media space. This is perhaps counterintuitive, given that the DMCA itself purports to support and encourage the deployment of DRM. But counterintuitive or not, this aspect seems to be present. And while it is far too early to pronounce a verdict on the legacy of these provisions of the DMCA, it may be that the lasting contribution of the DMCA to the copyright law is as a set of rules that stabilized, moderated, and encouraged relatively weak forms of DRM.[53]

IV. CONCLUSION: OR, HOW TO THINK ABOUT THE DMCA

I suggest that the conventional wisdom about the DMCA—as a simple, politically-driven "giveaway" of valuable rights to the content industries—misses both the real goal of the law as well as its importance in illuminating an emerging regulatory trend. The DMCA is fundamentally about the way that technology regulates, rather than a law about copyright. And understanding this point is important, both for our understanding of the copyright law, as well as for our thinking about the form and function of law in the modern regulatory environment. Indeed, the broader framework noted here is likely to have broad applicability to contexts beyond the digital content business. 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—such as the DMCA's anticircumvention provisions—that address both law and software will only increase.

53. Though the case is far from clear, there are good reasons to believe that "weak" forms of DRM might be a better solution than either "strong" or "no" forms. For an argument that the "leaky" nature of the copyright law is an essential feature, see Wagner, *supra* note 31, at 1010–16.