

ARTICLES

Pervasively Distributed Copyright Enforcement

JULIE E. COHEN*

ABSTRACT

In an effort to control flows of unauthorized information, the major copyright industries are pursuing a range of strategies designed to distribute copyright enforcement functions across a wide range of actors and to embed those functions within communications networks, protocols, and devices. Some of these strategies have received considerable academic and public scrutiny, but much less attention has been paid to the ways in which all of them overlap and intersect with one another. This Article offers a framework for theorizing that process. The distributed extension of intellectual property enforcement into private spaces and throughout communications networks can be understood as a new, hybrid species of disciplinary regime that locates the justification for its pervasive reach in a permanent state of crisis. This hybrid regime derives its force neither primarily from centralized authority nor primarily from decentralized, internalized norms, but instead from a set of coordinated processes for authorizing flows of information. Although the success of this project is not yet assured, its odds of success are by no means as remote as skeptics have suggested. Power to implement crisis management in the decentralized marketplace for digital content arises from a confluence of private and public interests and is amplified by the dynamics of technical standards processes. The emergent regime of pervasively distributed copyright enforcement has profound implications for the production of the networked information society.

TABLE OF CONTENTS

INTRODUCTION	2
I. THE STRATEGIES OF Pervasively Distributed Copyright ENFORCEMENT	3

* Professor, Georgetown University Law Center. © 2006, Julie E. Cohen. Thanks to Barton Beebe, Yochai Benkler, Bob Berring, Michael Birnhack, Dan Burk, Alex Cameron, Niva Elkin-Koren, Susan Freiwald, Brett Frischmann, Oscar Gandy, Tarleton Gillespie, Dan Hunter, Jerry Kang, Sonia Katyal, Mark Lemley, Jessica Litman, Clarisa Long, Michael Madison, David McGowan, Tom Nachbar, Ruth Okediji, Margaret Jane Radin, Pamela Samuelson, Seth Schoen, Paul Schwartz, Marc Spindelman, Peter Swire, Rebecca Tushnet, Fred von Lohmann, Phil Weiser, Tim Wu, Alfred Yen, participants in the New York University School of Law Colloquium on Innovation Policy, and participants in faculty workshops at the Georgetown University Law Center and the Harvard Law School for their helpful comments on earlier drafts, and to Andrew Crouse, Robert Dowers, Jonathan Putman, and Matthew Windsor for research assistance.

A.	SURFACE-LEVEL TECHNOLOGICAL RESTRICTIONS	4
B.	PRESSURE ON INDEPENDENT TECHNOLOGY DEVELOPERS	7
C.	“TRUSTED SYSTEMS” FUNCTIONALITY	11
D.	PRESSURE ON NETWORK GATEKEEPERS	14
E.	END-USER INITIATIVES	16
F.	RHETORICAL POSITIONING	18
II.	NORMAL DISCIPLINE IN THE AGE OF CRISIS	19
III.	CRISIS MANAGEMENT AND MARKET ORDERING	29
IV.	CRISIS MANAGEMENT AND THE PRODUCTION OF NETWORKED SPACE	37
V.	TAKING IMPERFECTION SERIOUSLY	43

INTRODUCTION

In an effort to control flows of unauthorized information, the major copyright industries are pursuing a range of strategies designed to distribute copyright enforcement functions across a wide range of actors and to embed those functions within communications networks, protocols, and devices. Some of these strategies have received considerable academic and public scrutiny, but much less attention has been paid to the ways in which all of them overlap and intersect with one another. That subject, I will argue, deserves far more careful consideration. The emerging regime of pervasively distributed copyright enforcement is not simply aimed at defining the boundaries of legal entitlements, nor at creating and rationalizing information flows within markets. It seeks to produce not only willing vendors and consumers, but also tractable ones, and it seeks these changes not merely at the behavioral level, but at the infrastructural level as well. The interplay between the strategies of pervasively distributed copyright enforcement thus frames important choices about the kind of information society we want to have.

Because pervasively distributed copyright enforcement represents more than just a change in markets, evaluating it requires that we look beyond literatures about markets to literatures about social ordering. The framework that I will suggest for theorizing pervasively distributed copyright enforcement as social ordering is informed substantially by the work of Michel Foucault and Anthony Giddens. Pervasively distributed copyright enforcement can be understood as a species of disciplinary regime similar in some respects to those that Foucault sought to understand. It is not, however, exactly like either of the disciplinary regimes identified by Foucault. Instead, it represents a new, hybrid type: a mode of normalized discipline that locates the justification for its pervasive reach in a

permanent state of crisis. This hybrid regime derives its force neither primarily from centralized authority nor primarily from decentralized, internalized norms, but instead from a set of coordinated processes for authorizing flows of information. Although the success of this project is not yet assured, the model of social change elaborated by Giddens suggests that its odds of success are by no means remote. Power to implement crisis management in the marketplace for digital content arises from the self-interested actions of market participants and is amplified by the dynamics of technical standards processes.

The emergent model of social ordering has profound implications for the production of the networked information society. Pervasively distributed copyright enforcement invades, disrupts, and casually rearranges the boundaries of personal spaces and of the intellectual and cultural activities played out within those spaces. This process threatens to produce, in turn, a larger geography of information space that is increasingly standardized. Finally, it promises to re-educate us to accept these changes as necessary, and eventually to perceive constraint and standardization as natural attributes of the information environment, if indeed we pause to think about them at all.

Important questions about the costs of this shift, and about alternatives, should not be swept aside by the rhetoric of exigency. Processes for authorizing flows of information are foundational to any networked information environment, but the precise forms that those processes will take are still undecided. This Article offers a plea for more careful attention to the experiential and political implications of a shift to crisis management, and to disciplinary alternatives that embrace unpredictability and imperfection.

I. THE STRATEGIES OF Pervasively Distributed Copyright Enforcement

In an effort to prevent online copyright infringement and protect established business models, the major copyright industries have developed and aggressively pursued a portfolio of strategies designed to implement a regime that I will call pervasively distributed copyright enforcement. These strategies rely on a range of tools including technologies that restrict the range of permitted information use, contractual regimes for authorizing “compliant” implementations of those technologies, legal prohibitions against interfering with the resulting techno-contractual regimes, other legal rules broadly distributing responsibility for policing communications networks, and publicly inculcated norms of appropriate user behavior. In aggregate, they are designed systematically to shift the locus of control over intellectual consumption and communication away from individuals and independent technology vendors and toward purveyors of copyrighted entertainment goods. Some of these strategies have received considerable public and scholarly attention, while others have not. Some are, and are intended to be, highly visible, while others are, and are intended to be, largely invisible to the public eye. Here I will be concerned less with the details of any particular strategy and more with their cumulative effect.

It is important to stress at the outset that each of the strategies that I will

describe is evolving and contested. Over time, some have waxed in importance while others have waned. What is presented here is a particular, increasingly unified regulatory agenda developed and steadily advanced by the content industries over the course of the past decade. This agenda is consistent with, and is intended to cement, the larger agenda of commodification of information goods pursued by these industries. Whether pervasively distributed copyright enforcement will become reality, and to what extent, are questions that are yet to be determined. Many technically sophisticated observers believe that uncontrolled “darknets” will always evade the content industries’ reach.¹ I take no position on whether that is so; as I will show, the possibility of digital *samizdat* does not undercut, but instead reinforces, the argument presented here, which concerns the baseline held out to the average user of digital information as the alternative to lawlessness.

The strategies of pervasively distributed copyright enforcement may be provisionally categorized into six groups, according to the behaviors that each group primarily targets. Each set of enforcement strategies is internally heterogeneous, by which I mean both that each employs multiple regulatory modalities and that each targets and seeks to stabilize relations among a variety of actors and objects.² In this respect my methodology differs from the prevailing approach within the scholarly literatures on copyright and cyberspace law, which classifies regulatory strategies according to the four-part taxonomy of regulatory modalities developed by Lawrence Lessig.³ As I hope to demonstrate, an analysis of copyright enforcement that analyzes these modalities separately would not capture the ways in which they intersect.

A. SURFACE-LEVEL TECHNOLOGICAL RESTRICTIONS

The first set of strategies revolves around what I will call “surface-level” implementation of automated restrictions on digital content. These restrictions—variously known as copy-protection technologies, technical protection measures (TPMs), and digital rights management (DRM)—operate at the level of individual media files, and restrict the actions that users may take with the files. Because they operate at surface level, implementing these restrictions does not require the direct involvement of computer operating system developers, micro-processor companies, or even middleware vendors. Instead, surface-level TPMs

1. See Peter Biddle et al., *The Darknet and the Future of Content Distribution*, in PROCEEDINGS OF THE 2002 ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT (2002), <http://crypto.stanford.edu/DRM2002/darknet5.doc>; see also Fred von Lohmann, *Measuring the Digital Millennium Copyright Act Against the Darknet: Implications for the Regulation of Technological Protection Measures*, 24 LOY. L.A. ENT. L. REV. 635 (2004).

2. See generally John Law, *Technology and Heterogeneous Engineering: The Case of Portuguese Expansion*, in THE SOCIAL CONSTRUCTION OF TECHNOLOGICAL SYSTEMS 111, 111–34 (Wiebe Bijker et al. eds., 1987) (arguing that technology-based regulation operates by enrolling heterogeneous elements into coordinated networks).

3. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 85–95 (1999); see, e.g., R. Polk Wagner, *On Software Regulation*, 78 S. CAL. L. REV. 457 (2005).

are developed and implemented at the application level and in freestanding consumer electronics equipment via licensing processes coordinated by copyright interests and their designated technology partners. Within these technical-contractual regimes, the relevant technical standards are held as trade secrets. Licensees recruited into these regimes must agree to preserve secrecy, and their implementations of the standards must satisfy associated criteria of robustness.⁴

So far, surface-level protection strategies have produced some notable failures, but also some notable successes. The most highly publicized and widely criticized efforts to implement surface-level technological restrictions have occurred within the recording industry. Over the past few years, the major industry players have experimented with a variety of copy-protection technologies for CD releases. Because copy-protected CDs typically will not play on the full range of equipment now used for playing back unprotected CDs, music consumers have resisted them.⁵ New copy-protections have been hacked almost as rapidly as they have appeared, and industry efforts to develop a universal, more robust standard for technical protection of music files have failed. Ventures in online music distribution have deployed surface-level protection strategies more successfully, however. Most of these services, including Apple's much-hyped iTunes program, offer downloads in proprietary formats tied to specific digital music devices.⁶

A more successful example of surface-level technological restriction is the encryption system built into DVD players and incorporated in all prerecorded DVDs. This encryption system prevents copying and also incorporates a system of "region coding" designed to preserve geographic price discrimination. Both the copy-protection and region-coding features of the system are enforced by technical rules that prohibit play on any noncompliant DVD player.⁷ The

4. See TARLETON GILLESPIE, *WIRED SHUT: COPYRIGHT AND THE RE-ALIGNMENT OF DIGITAL CULTURE* ch. 8 (forthcoming 2007).

5. Some early versions of surface-level protection prevented playback using a personal computer or accompanying peripheral device. See Amy Harmon, *CD-Protection Complaint Is Settled*, N.Y. TIMES, Feb. 25, 2002, at C8; P.J. Huffstutter & Jon Healey, *Suit Filed Against Record Firms*, L.A. TIMES, June 14, 2002, at C3; Brenda Sandburg, *Milberg Weiss Files Suit Over CDs With No-Copy Technology*, RECORDER, June 17, 2002, at 1. More recent versions allow computer playback using approved media players that incorporate the copy-protection. As an additional concession to wary consumers, the technology permits a limited amount of home copying, but the record labels have disclosed that planned upgrades will substantially reduce that amount. See John Borland, *Copy-Blocked CD Tops U.S. Charts*, CNET NEWS.COM, June 17, 2004, <http://news.com.com/2100-1027-5238208.html>; John Borland, *Labels to Dampen CD Burning?*, CNET NEWS.COM, June 2, 2004, <http://news.com.com/2100-1027-5224090.html>.

6. See Peter Lewis, *Drop a Quarter in the Internet*, FORTUNE, Mar. 22, 2004, at 56; Rob Pegoraro, *Apple Comes Closer to Perfect Pitch*, WASH. POST, May 4, 2003, at F07, available at <http://www.washingtonpost.com/ac2/wp-dyn/A8159-2003May2>; see also Scott Banerjee & Brian Garrity, *Napster, Apple in Campus Deals*, BILLBOARD, July 31, 2004, at 6 (describing several major universities' entry into partnership agreements with particular digital music services).

7. See Matt Lake, *How It Works: Tweaking Technology to Stay Ahead of the Film Pirates*, N.Y. TIMES, Aug. 2, 2001, at G9; Doug Mellgren, *Acquittal in DVD Decoding: Norwegian Teen Created Program So He Could View Film on Computer*, CHARLOTTE OBSERVER, Jan. 8, 2003, at 3D; John

technical standards were developed by a consortium of the major studios and are currently administered and enforced by a private membership association, the DVD Copy Control Association (DVD-CCA), that licenses the technology.

The success of the technical-contractual regime administered by the DVD-CCA is not due to its technical efficacy in any absolute sense. The copy-protection algorithm, known as the Content Scramble System (CSS) has been broken, and the decryption algorithm, known as DeCSS, is widely available on the Internet if one knows where to look. Most people don't do this, though, and this appears to be a function of two related factors: the technology's universality and its perceived normalcy. Because the deliberately designed limitations have been in place from the moment that DVD players were first marketed to consumers, the operation of the regime administered by the DVD-CCA is effectively invisible to end users; it is "just the way things are."

Surface-level restrictions might, but need not, incorporate surveillance functionality that reports back to the content provider about users' activities. So far, surveillance seems to have occurred principally for purposes more directly connected to marketing than to enforcement. An early version of the RealNetworks media player collected and reported information about the system on which it was installed, including the number and titles of music files stored on the system and the types of portable music players installed.⁸ The "SmartDownload" software included with the 1998 version of Netscape's Communicator web browser recorded every web site visited by users and transmitted that information back to Netscape.⁹ Both of these incidents provoked intense public outcry and culminated in expensive litigation asserting a variety of privacy claims. Perhaps for this reason, surveillance does not appear to play a role in many current surface-level enforcement initiatives, which focus more narrowly on preventing unauthorized actions.

Surface-level restrictions also may incorporate other, more aggressive types of functionality. In October 2005, a researcher discovered that media player software bundled with a number of Sony's recent CD releases was surreptitiously installing third-party rights management software on users' computers and employing a technique known as a rootkit, more commonly used by spammers and spyware distributors, to conceal that fact.¹⁰ After a period of intense activity, security researchers determined that in addition to enforcing copying restrictions encoded on the Sony CDs, the software also interfered with the ripping of unprotected media files from other sources. In addition, the

Borland, *Studios Race to Choke DVD Copying*, CNET NEWS.COM, Feb. 4, 2002, <http://news.com.com/2100-1023-828449.html>.

8. Greg Miller, *RealNetworks Breached Privacy, 3 Suits Contend*, L.A. TIMES, Nov. 11, 1999, at C1.

9. See *Specht v. Netscape Commc'ns Corp.*, 150 F. Supp. 2d 585, 587 (S.D.N.Y. 2001), *aff'd*, 306 F.3d 17, 35 (2d Cir. 2002) (holding that clickwrap agreement giving consent to the monitoring was unenforceable because of curable defects in contract formation).

10. See Matthew Fordhal, *Sony Patch Reveals Its Anti-Piracy Files on PCs*, WASH. POST, Nov. 3, 2005, at D5; Mark's Sysinternals Blog, <http://www.sysinternals.com/blog/> (Oct. 31, 2005, 11:04).

design of the software afforded a hidden “back door” to users’ computer systems for viruses and other forms of malware. No uninstall utility was included with the software, and attempting to remove the files from an affected computer could corrupt its operating system, disabling the CD drive entirely.¹¹ In the ensuing uproar, Sony and its third-party vendor released patches to enable removal of the software and recalled the affected CDs from stores.¹² However, Sony did not pledge to forego surreptitious technical protection efforts in the future, and several other major entertainment providers vigorously asserted both the need and the right to employ such efforts. Spyware techniques are currently under intense scrutiny by Congress, but the major entertainment industries have urged that any law enacted to regulate spyware should exempt software installed for rights management purposes.¹³

B. PRESSURE ON INDEPENDENT TECHNOLOGY DEVELOPERS

A second set of strategies for pervasively distributed copyright enforcement targets third-party technology companies whose products and services are perceived to facilitate particularly high levels of infringement. In broad brush, this campaign has two complementary goals. First, it seeks to keep protected content protected. The primary vehicle for accomplishing this goal is the Digital Millennium Copyright Act (DMCA),¹⁴ which penalizes providers of technologies that enable users to gain unauthorized access to protected content. Second, it seeks to minimize the availability of tools for reproducing, distributing, and manipulating unprotected content. Equipment and services that give users this freedom—including digital video recorders, digital music players, and CD and DVD burners—work at cross purposes with the effort to shift the market toward protected content. In an effort to assert control over these segments of the technological marketplace, the entertainment industries have invoked a set of doctrines within copyright law that create liability for facilitating an unacceptably high degree of copyright infringement.

The DMCA advances the goal of keeping protected content protected in three interrelated ways: It prohibits circumvention of technological measures that effectively control access to copyrighted works, bans the manufacture and

11. See Brian Krebs, *Study of Sony Anti-Piracy Software Triggers Uproar*, WASH. POST, Nov. 3, 2005, at D05.

12. See Fordhal, *supra* note 10; Jefferson Graham, *Sony to Pull Controversial CDs, Offer Swap*, USA TODAY, Nov. 14, 2005, at 1B. To add injury to insult, researchers soon discovered that the removal tool created even more “gaping” system security holes. Posting of J. Alex Halderman & Ed Felten to Freedom to Tinker, *Sony’s Web-Based Uninstaller Opens a Big Security Hole; Sony to Recall Discs*, <http://freedom-to-tinker.com/> (Nov. 15, 2005, 7:07).

13. For one such provision, see Spy Act, H.R. 29, 109th Cong. § 5(b)(2) (2005); see also Todd Martens & Brian Garrity, *Consumers Sing DRM Blues*, BILLBOARD, Nov. 12, 2005, at 6 (quoting industry sources as confirming that “hiding software on computers is standard” because “the object is to make it more difficult to circumvent”).

14. Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, § 103, 112 Stat. 2860, 2863–76 (1998) (codified at 17 U.S.C. §§ 1201–1202 (2000)).

distribution of technologies that might enable copyrighted content to be stripped free of its protective coating, and forbids the knowing removal of “copyright management information,” including information about the terms and conditions for use of the work.¹⁵ The DMCA was enacted as part of U.S. accession to a 1996 treaty that requires effective legal protection for technological measures applied to copyrighted works, and has served as a model for implementing legislation in other countries.¹⁶ The U.S.-based entertainment industries also have spearheaded an effort to export the model of the DMCA to other countries via bilateral trade agreements.¹⁷

DMCA-style laws do not physically or electronically prevent the spread of unprotected content or circumvention tools, and for that reason some critics consider them ineffective. For example, the DMCA did not prevent the development and widespread Internet distribution of DeCSS, the unauthorized program that decrypts prerecorded DVDs. Even after successful and widely-publicized litigation against several high-profile U.S. distributors of DeCSS, both the algorithm and movies decrypted with it remain widely available.¹⁸ Although the costs of violating DMCA-style prohibitions may be trivial from an individual user’s perspective, however, they are far more significant for would-be legitimate providers of digital media equipment and services. The content industries have filed a steady progression of DMCA lawsuits against technology companies whose products interfered with technological protection measures.¹⁹ The potential costs of DMCA litigation also have affected independent researchers who study the technological systems that the DMCA protects; many of these researchers report having changed their research programs to avoid legal conflict.

15. *Id.*

16. World Intellectual Property Organization Copyright Treaty art. 11, Dec. 20, 1996, 11 Stat. 2860, 36 I.L.M. 65 (1997). Some commentators have argued that the treaty’s requirements would be satisfied by substantially less draconian restrictions. *See, e.g.*, Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 530–32 (1999). The point seems on the way to becoming moot, however.

17. *See* U.S.-Morocco Free Trade Agreement, U.S.-Morocco, art. 15.8, June 15, 2004, 44 I.L.M. 544 (2005); U.S.-Bahrain Free Trade Agreement, U.S.-Bahr., art. 14.4(7)–(8), Sept. 14, 2004, 44 I.L.M. 544 (2005); Australia-U.S. Free Trade Agreement, U.S.-Austl., art. 17.4(7)(a), May 18, 2004, 43 I.L.M. 1248 (2004); U.S.-Chile Free Trade Agreement, U.S.-Chile, art. 17.7(5)–(6), June 6, 2003, 42 I.L.M. 1026 (2003); U.S.-Singapore Free Trade Agreement, U.S.-Sing., art. 16.4(7)(a), May 6, 2003, 42 I.L.M. 1026 (2003); U.S.-Jordan Free Trade Agreement, U.S.-Jordan, art. 4(13), Oct. 24, 2000; *see also* Free Trade Area of the Americas Draft Agreement ch. 20, art. 22, Nov. 21, 2003.

18. *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 332 (S.D.N.Y. 2000), *aff’d sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); *see also* DVD Copy Control Ass’n v. Bunner, 116 Cal. App. 4th 241, 255 (2004) (denying injunctive relief on trade secrecy grounds against web site operator who posted DeCSS because DeCSS was widely available at the time the lawsuit was filed and therefore the information it contained could no longer qualify as a trade secret).

19. *See* Paramount Pictures Corp. v. 321 Studios, No. 03-CV-8970 (RO), 2004 WL 402756 (S.D.N.Y. Mar. 3, 2004); 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004); RealNetworks, Inc. v. Streambox, Inc., No. C99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000).

Technologies that allow copying, manipulation, and distribution of unprotected content do not implicate the DMCA; these technologies and related services violate the law only if there is a sufficiently direct link to copyright infringement under either of two theories of indirect liability. By analogy to the common law doctrine of respondeat superior, a third party is vicariously liable for copyright infringement if it receives a direct financial benefit from the infringement and has the right and opportunity to control the infringing conduct.²⁰ Alternatively, a third party is considered a contributory copyright infringer if, with knowledge of the infringing conduct, it materially facilitates or participates in the conduct.²¹ For many years, this doctrinal structure effectively shielded technology providers from liability. The provider of standalone equipment, such as a CD burner, typically had neither an ongoing right to control uses of its products nor knowledge of specific acts of infringement that occurred after sale. Equipment providers did know that their products would be used to infringe copyrights, but in *Sony Corp. of America v. Universal City Studios, Inc.* the Supreme Court ruled that constructive knowledge of infringement could not be imputed to an equipment provider as long as the product was “capable of substantial noninfringing uses.”²²

In a carefully designed litigation campaign, the entertainment industries have eroded the certainty afforded by the *Sony* safe harbor. The campaign targeted a set of particularly unsympathetic defendants: providers of p2p file-sharing software that enabled millions of users to exchange digital media files directly with one another. In a series of widely-publicized lawsuits against the p2p providers known as Napster, Aimster, and Grokster, the industry plaintiffs emphasized both the sheer volume of infringement and the defendants’ failure to implement design changes that might minimize infringement. This strategy produced a circuit split on the proper interpretation of *Sony*. Under one interpretation, a contributory infringement defendant need only show that its product is capable of future noninfringing uses that are qualitatively substantial.²³ Under the other, it must show current, quantitatively substantial noninfringing uses, and also must show that there were not reasonable steps it could have taken to reduce the level of infringement.²⁴ Many technology developers can pass the first test; fewer can survive the second. When the Supreme Court granted review in *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster*,²⁵ technology developers hoped at minimum for a clearer statement of the applicable rule. Instead, the

20. See *Gershwin Publ’g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971); *Shapiro, Bernstein & Co. v. H.L. Green Co.*, 316 F.2d 304, 307 (2d Cir. 1963).

21. See *Gershwin Publ’g*, 443 F.2d at 1162.

22. *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984).

23. See *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd.*, 380 F.3d 1154, 1162–66 (9th Cir. 2004), *vacated*, 125 S. Ct. 2764, 2789–92 (2005); *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1020–22 (9th Cir. 2001).

24. See *In re Aimster Copyright Litig.*, 334 F.3d 643, 649–53 (7th Cir. 2003), *cert. denied sub nom. Deep v. Recording Indus. Ass’n of Am.*, 540 U.S. 1102 (2004).

25. *Metro-Goldwyn-Mayer Studios, Inc.*, 125 S. Ct. at 2779–80.

Court declined to resolve the disagreement, and compounded the uncertainty by articulating an alternative basis for contributory infringement liability based on intent to induce infringement. The contours of the new inducement test are poorly defined. In particular, the Court's opinion is vague on the critical question of a technology developer's design obligations to minimize infringement.²⁶ After *Grokster*, it is unclear what a developer must show to avoid liability under either theory.

The debate about the proper interpretation of *Sony* and *Grokster*, moreover, has overlooked the extent to which developers of networked communications technologies may be ineligible to invoke *Sony*'s protection. In the case of products that incorporate a degree of ongoing networked control, a copyright plaintiff need not resort to arguing constructive knowledge or bad intent. If ongoing networked control enables specific knowledge of infringing conduct and affords an opportunity to prevent or minimize it, liability will arise under the traditional theory of contributory infringement, and possibly under the theory of vicarious liability as well.²⁷ Many digital media technologies incorporate elements of ongoing networked control for technical and business reasons such as delivery of software updates and provision of technical support. For these products and services, there are thus three separate and independent ways in which a copyright plaintiff can establish the requisites of a contributory liability claim.

All of these potential sources of legal liability cast a pall over innovation in high-technology markets that reaches far beyond providers of p2p file-sharing technologies. For technology developers, the case of the ReplayTV digital video recorder provides an object lesson in the risks of incurring the content industries' displeasure. The ReplayTV gave users the ability to skip commercials automatically upon playback and the ability to share recorded programming with other ReplayTV users. A group of movie and television studios sued the ReplayTV's manufacturer, SonicBlue, for enabling infringement of their copyrights, and embarked upon a lengthy and expensive discovery campaign.²⁸ SonicBlue eventually filed for bankruptcy and sold its ReplayTV technology and business to a major consumer electronics company.²⁹ ReplayTV's new owners promptly agreed to remove the two features that were the subject of the lawsuit.³⁰ In the wake of this victory, the studios stepped up pressure on TiVo, the leader in the digital video recorder market, to modify its product to make commercial-skipping more difficult. Eventually, TiVo announced that it would comply with these requests.³¹

26. *Id.* at 2781 & n.12.

27. See *Grokster*, 380 F.3d at 1162–66; *Aimster*, 334 F.3d at 649, 653.

28. See Farhad Manjoo, *Sonicblue Freed From Monitoring*, WIRED.COM, June 3, 2002, <http://www.wired.com/news/business/1,52934-0.html>.

29. See Eric A. Taub, *ReplayTV's New Owners Drop Features That Riled Hollywood*, N.Y. TIMES, July 21, 2003, at C3; Jim Hu, *Sonicblue Seeks Bankruptcy Protection*, CNET NEWS.COM, March 21, 2003, <http://news.com.com/2100-1047-993647.html>.

30. See Taub, *supra* note 29.

31. See Gina Piccalo, *TiVo Will No Longer Skip Past Advertisers*, L.A. TIMES, Nov. 17, 2004, at A1.

Finally, the entertainment industries also have used indirect copyright infringement lawsuits to target entities that provide essential business services to recalcitrant independents. In two highly-publicized lawsuits following its Napster victory, the recording industry has sought to call Napster's financial backers to account for their purported complicity in Napster's violations.³² The same federal district judge who presided over the Napster litigation rejected the financiers' arguments that this would amount to creation of a novel and chilling theory of "tertiary liability" for copyright infringement and ruled that the lawsuit could proceed to the discovery phase.³³ In another court, an online pornographer sued an age verification service used by competitors that made copied, infringing materials available to their subscribers.³⁴ Also worth noting in this category is a malpractice lawsuit by failed Internet music venture MP3.com against its own legal counsel, premised on the theory that MP3.com's business model was so clearly infringing that its lawyers' advice to proceed with the business model fell below the generally accepted standard of professional care.³⁵ So far these lawsuits have produced mixed results, and judges uniformly have held that the traditional requirements for indirect liability must be met. Once again, however, this litigation strategy is not designed simply to produce favorable law on the books, but more generally to cause venture capitalists and service firms to adopt a more cautious stance toward their dealings with maverick technology companies. Whether it has succeeded in that regard is harder to determine.

C. "TRUSTED SYSTEMS" FUNCTIONALITY

The third set of strategies for pervasively distributed copyright enforcement seeks to move automated enforcement functions progressively deeper into the logical and physical layers of the user's electronic environment. Such "trusted systems" efforts are, and are designed to be, far more impervious to hacker workarounds. They are also far more inhospitable to unauthorized technologies that an independent third party might seek to market. They are, however, far more complicated to implement. Successfully operationalizing trusted systems functionality across the broad range of personal computing and consumer

32. See Roger Parloff, *Killer App: Thanks to Its Ballyhooed Napster Alliance, Bertelsmann Faces More than \$17 Billion in Copyright Lawsuits*, FORTUNE, Sept. 1, 2003, at 111; Dan Primack, *Paying for Downloading Music: Hummer Winblad Is Still Dealing with the Consequences of Its \$15 Million Investment in Napster*, VENTURE CAP. J., Mar. 1, 2004, available at 2004 WLNR 56830.

33. See UMG Recordings, Inc. v. Bertelsmann AG, 222 F.R.D. 408 (N.D. Cal. 2004) (order denying motion to dismiss).

34. See Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002); see also John Schwartz, *The Pornography Industry vs. Digital Pirates*, N.Y. TIMES, Feb. 8, 2004, at 31 (describing other lawsuits by Perfect 10). The parties reached a confidential settlement.

35. See Sonia K. Katyal, *A Legal Malpractice Claim by MP3.com: In the Changing Area of Cyberlaw, Is a Crystal Ball Necessary to Avoid Liability?*, FINDLAW'S WRIT, Feb. 7, 2002, http://writ.news.findlaw.com/commentary/20020207_katyal.html. The case was settled by confidential agreement.

electronic equipment now in use requires the cooperation of major sectors of the software, computer and communications industries. So far, the track record of these initiatives is mixed.

A variety of trusted systems projects are currently underway. Some focus on implementing controls at the operating system layer, while others seek to hard-wire trusted systems functionality into every kind of equipment that users might employ to access copyrighted content. Microsoft's internal project, which has undergone several name changes over the years, is perhaps the most highly publicized example of such an initiative. Designated as a security system, its core functionality revolves around standards for authenticating "trusted" programs and files. Although some standards would be set by users, others would be set to the specifications of Microsoft and its licensing partners, which could include providers of a broad range of copyrighted content.³⁶ Intel's LaGrande project is exploring the inclusion of control-enabling standards in the microprocessors used in personal computer systems.³⁷ Other efforts to develop and implement trusted systems controls are more collaborative, and include: the Trusted Computing Group ("TCG"),³⁸ a joint venture of Microsoft, Intel, AMD, IBM, Hewlett Packard, Sony, and Sun Microsystems that seeks to coordinate development of trusted systems standards for personal computing platforms; the 5C alliance,³⁹ a joint venture of Hitachi, Intel, Matsushita, Sony, and Toshiba that seeks to develop trusted systems standards for digital broadcasting; the Digital Media Project⁴⁰ and the Coral Consortium,⁴¹ both of which seek to develop standards for moving protected content across different consumer platforms; and the Copy Protection Technical Working Group,⁴² a more broad-based industry effort to coordinate all types of trusted systems research and development.

36. See Andy Dorman, *Trusted Computing Architectures*, NETWORK MAG., July 1, 2005, at 53; Neil McIntosh, *Online: Old Bill's Police Tactics*, THE GUARDIAN, July 4, 2002, at 7; Michael J. Miller, *Hands on with the Next Windows: Longhorn No Longer. Windows Vista Is Now Looming Large*, PC MAG., Sept. 6, 2005, at 14; Arif Mohamed, *Who Can You Trust?*, CPTR. WEEKLY, Apr. 26, 2005, at 40; Mary Jo Foley, *Microsoft: 'Palladium' Is Still Alive and Kicking*, EXTREME TECH.COM, May 5, 2004, <http://www.extremetech.com/article2/0,1558,1586312,00.asp>; Robert Lemos, *What's in a Name? Not Palladium*, CNET NEWS.COM, Jan. 24, 2003, http://news.com.com/2100-1001_3-982127.html.

37. See Chris Gaither, *Intel Chip to Include Antipiracy Features, Some Still Fear Privacy of Users Will Be Violated*, BOSTON GLOBE, Sept. 10, 2002, at C3; Greg Sandoval & Matthew Fordhal, *Apple's Chip Switch Could Open New Window for Macs*, TECH. REVIEW, June 13, 2005, http://www.techreview.com/articles/05/06/ap/ap_061305.asp; Nick Stam, *Inside Intel's Secretive 'LaGrande' Project*, EXTREME TECH.COM, Sept. 19, 2003, <http://www.extremetech.com/article2/0,3973,1274197,00.asp>; Nick Stam, *Tomorrow's CPUs Today*, EXTREME TECH.COM, July 20, 2005, <http://www.extremetech.com/article2/0,1697,1839315,00.asp>; see also John Clyman, *Making Computing Trustworthy*, PC MAG., Nov. 11, 2003, at 97 (discussing both LaGrande and Microsoft's NGSCB); Alexander Wolfe, *Up the Value Chain—Systems Builders Seek Technology Edge in Bid to Differentiate*, VARBUSINESS, May 16, 2005, at 37 (noting that the new Microsoft and Intel technologies are designed to be compatible).

38. Trusted Computing Group, <http://www.trustedcomputinggroup.org>.

39. See HITACHI, LTD. ET AL., 5C DIGITAL TRANSMISSION CONTENT PROTECTION WHITE PAPER (1998), http://www.dtcp.com/data/wp_spec.pdf; Digital Transmission Licensing Administration, <http://www.dtcp.com/>.

40. Digital Media Project Website, <http://www.dmpf.org>.

41. Coral Consortium, <http://www.coral-interop.org>.

42. Copy Protection Technical Working Group, <http://cptwg.org>.

The most hotly debated aspect of trusted systems strategies for pervasively distributed copyright enforcement has concerned the role of government in coordinating their implementation. Although the entertainment industries have vigorously asserted that they are best positioned both to develop the relevant standards and to establish procedures for licensing compliant implementations, they have repeatedly failed to secure a private consensus on these and other issues. The asserted goal of building a single standard into the network has been stymied by the parties' distrust of one another, and by inter-industry struggles for market position. As a result, they have turned to government authorities to solve bargaining breakdown problems.

Whether and how governments will become involved in trusted systems development are unresolved questions. In the U.S., the entertainment industries have repeatedly requested the enactment of laws mandating the development and adoption of content protection standards. An initial effort to secure a broad mandate covering all computing and consumer electronics equipment failed when the technology industries refused to support it.⁴³ In the wake of this failure, however, both content and technology industries have supported narrower proposals for government intervention. In the 2005–06 legislative session, Congress is considering a proposal to require a “broadcast flag” for digital television content, another proposal to create a parallel regime for digital audio broadcasts, and a third proposal that would mandate watermarking of broadcast content to prevent broadcasts recorded using analog technologies from being digitized.⁴⁴ Meanwhile, the FCC is conducting its own audio broadcast flag rulemaking, and has already issued a rule establishing content protection requirements for content distributed via cable.⁴⁵ The European Commission is also considering strategies for encouraging the development of trusted systems technologies.⁴⁶

The question whether the standards underlying all of these initiatives will be

43. See Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong. (2d Sess. 2002).

44. See Audio Broadcast Flag Licensing Act of 2006, H.R. 4861, 109th Cong. (2d Sess. 2006); Digital Transition Content Security Act of 2005, H.R. 4569, 109th Cong. (1st Sess. 2005); Sen. Gordon Smith, Digital Content Protection Act of 2006, 109th Cong. (1st Sess. 2005) (discussion draft), http://www.eff.org/broadcastflag/dcp_act_2006.pdf.

45. See Fed. Comm'n Comm'n (FCC), Further Notice of Proposed Rulemaking and Notice of Inquiry, No. 04-99 (Apr. 15, 2004), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-99A4.pdf; Commercial Availability of Navigation Devices and Compatibility Between Cable Systems and Consumer Electronics Equipment, 68 Fed. Reg. 66,728 (Nov. 28, 2003) (codified at 47 C.F.R. pts. 15, 76). In 2003, the FCC issued a rule intended to coordinate the development of a broadcast flag for digital television, but opponents of the regulation convinced a court to strike down the rule on jurisdictional grounds. See *Am. Library Ass'n v. FCC*, 406 F.3d 689 (D.C. Cir. 2005); see also Notice of Proposed Rulemaking, 68 Fed. Reg. 67,624 (Dec. 3, 2003); Digital Broadcast Content Protection, 68 Fed. Reg. 67,599 (Dec. 3, 2003) (codified at 47 C.F.R. pts. 73, 76); Report and Order and Further Notice of Proposed Rulemaking, *In re Digital Broadcast Content Protection*, 18 F.C.C.R. 23,550 (2003). The legislative proposal now under discussion would cure the jurisdictional defect and reinstate the FCC's broadcast flag rule.

46. See HIGH LEVEL GROUP ON DIGITAL RIGHTS MGMT., FINAL REPORT (2004), http://europa.eu.int/information_society/eeurope/2005/all_about/digital_rights_man/doc/040709_hlg_drm_2nd_meeting_final_report.pdf.

open or proprietary also remains unanswered. In the U.S., the major entertainment and technology companies have almost uniformly supported proprietary standards. In Europe, in contrast, an inter-industry working group has recommended that the government encourage the development of open standards for content protection.⁴⁷ There appear to be two reasons for this transatlantic divergence. First, the working group convened by the European Commission to study content protection issues included not only representatives of the content industries, but also public broadcasters and consumer groups. Second, the European technology companies were still smarting over their exclusion from U.S.-Japanese joint ventures such as the TCG and the 5C alliance.

Exclusive focus on the question of technology mandates, however, ignores the extent to which trusted systems initiatives continue to move forward via private standards processes. In particular, the demand for trusted systems functionality leverages a more general and growing popular and commercial demand for security against viruses, spyware, and spam.⁴⁸ As Jonathan Zittrain describes, the demand for security in online transactions is catalyzing a wide variety of design efforts aimed at making the ends of the network more amenable to control.⁴⁹ While the marketplace response to surface-level technological protection has been equivocal, demand for robust protection against malware is strong. Many innovations directed principally at security concerns can be adapted for copyright enforcement purposes, and many innovations directed principally at copyright enforcement can be described as targeting generalizable “security” concerns. One example of a multipurpose “security” technology is the newest version of the Internet Protocol, IPv6, which includes a so-called “stateful” mode that facilitates persistent identification of Internet users.⁵⁰ This technology was designed to enable secure transactions, and it can be adapted for copyright enforcement purposes as well.

D. PRESSURE ON NETWORK GATEKEEPERS

The fourth set of strategies for pervasively distributed copyright enforcement targets third-party providers of network services, such as ISPs and search engines, that play a vital role in the distribution of online communication, including both protected and unprotected content. ISPs serve as gatekeepers for

47. *See id.* at 13.

48. It also leverages a demand for traceability in the interest of “homeland security,” but here the overlap is more complicated. Some aspects of this overlap are considered in Part III, *infra*.

49. *See* Jonathan Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974 (2006).

50. *See* Internet Engineering Task Force, RFC 3041, *Privacy Extensions for Stateless Autoconfiguration in IPv6*, <http://www.ietf.org/rfc/rfc3041.txt?number=3041>. The Internet Engineering Task Force recommends implementation of IPv6 in a way that allows individual users to decide whether to enable or disable this mode, but it cannot require this. *See id.*; *see also* Peter Sevcik, *Who Will Control Tomorrow's Internet?*, BUS. COMM. REV., Sept. 1, 2003, at 8 (describing projects under way at Microsoft, Sony, and Panasonic to build permanent addressing capability into their products). In any event, a content provider can require that the stateful mode be enabled before it transfers digital content.

most online conduct by users, while search engines play an analogous gatekeeping role in the processes of online search and retrieval. In 1998, as part of the DMCA, the U.S. copyright industries won passage of legislation establishing a “notice and takedown” procedure under which both types of service providers may maintain immunity from monetary liability by promptly removing material called to their attention by copyright owners.⁵¹ Like the other provisions of the DMCA, this provision too has served as a model for legislation in other countries. Formally, compliance with the notice and takedown procedure is optional. Because the notice of infringement also creates the factual predicate for contributory infringement liability, however, service providers have a pressing incentive to comply despite (or perhaps because of) the fact that the legal predicate for the contributory liability of online service providers still has not been definitively established by any court.⁵² A recent quantitative study of takedown notices served on online service providers found that over thirty percent presented questionable claims of infringement and that many more were technically flawed.⁵³

Nonprofit educational institutions that function as ISPs for their students and staff have posed especially difficult problems for the strategy of recruiting gatekeepers as copyright enforcers. When the copyright and Internet service industries negotiated the compromise that became the notice and takedown regime, these institutions, which have considerable political power of their own, sought and won additional special protections. Most significantly, actions of users at nonprofit educational institutions may not be attributed to the institution unless it is on notice of a pattern of infringing conduct. The content industries have stepped up efforts to provide such notice. They also have sent letters to the presidents of U.S. colleges and universities requesting that they monitor student Internet accounts to detect peer-to-peer file trading activities, and have provided universities with automated tools for processing takedown notices and disabling student access to peer-to-peer networks.⁵⁴ Some universities have resisted these overtures, but some have accepted them.

The DMCA’s notice and takedown provisions do not apply to service providers based outside the U.S., nor do they apply to entities that merely serve as passive conduits for Internet traffic routed from non-U.S. locations. Nonethe-

51. Digital Millennium Copyright Act, Pub. L. No. 105-304, § 502, 112 Stat. 2860, 2905–16 (1998) (codified at 17 U.S.C. § 512 (2000)).

52. For an illuminating discussion of service provider incentives to police online copyright infringement, see Assaf Hamdani, *Who’s Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901 (2002).

53. Jennifer Urban & Laura Quilter, *Efficient Process or “Chilling Effects”? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621 (2006).

54. See Am. Council on Educ., *Higher Education Associations and the Creative Content Community Letters on P2P Piracy*, ACENET, Oct. 8, 2002, <http://192.111.222.22/washington/letters/2002/10october/copyright.cfm>; Stefanie Olsen, *Hollywood’s New Lesson for Campus File Swappers*, CNET NEWS.COM, Apr. 19, 2004, http://news.com.com/2100-1027_3-5194341.html (describing implementation of protective policies at U.C.L.A. and the University of Florida).

less, the statute contains a separate, little-discussed provision authorizing injunctive relief against a service provider to block access to a specific location outside the U.S.⁵⁵ In at least one case, the entertainment industries have successfully invoked this provision to encourage “conduit” service providers to close national borders to allegedly infringing traffic. In 2002, the recording industry sued to require providers of Internet backbone service to block access to Listen4Ever, a China-based web site offering copyrighted music files for download. The Listen4Ever site “disappeared” shortly thereafter, and the industry dismissed the suit.⁵⁶

E. END-USER INITIATIVES

The fifth set of strategies for pervasively distributed copyright enforcement consists of efforts directed at changing end-user behavior. The recording and motion picture industries have mounted a concerted campaign to convince individual users that unauthorized use of their copyrighted content is too risky. Following a template established by the software industry for corporate users, the recording industry briefly experimented with an amnesty program designed to encourage users to “come clean” and pledge to change their ways. Few users took advantage of this program, however, and a consumer group filed a lawsuit alleging that elements of it were deceptive, so the industry abandoned it.⁵⁷ Since then, the two industries have employed more draconian tactics.

The principal element in the entertainment industries’ enforcement campaign against individual end users consists of highly publicized waves of civil lawsuits. The Recording Industry Association of America and the Motion Picture Association of America have filed thousands of so-called “John Doe” lawsuits against anonymous file traders.⁵⁸ This procedural tactic enables them to request

55. See 17 U.S.C. § 512(j)(1)(B)(ii) (2000).

56. See Kate Bulkley, *New Media: Fair Play or Foul?*, THE GUARDIAN (London), Aug. 26, 2002, at 20; Alex Pham, *Tactics Toughen on Music Piracy*, L.A. TIMES, Aug. 21, 2002, at C1; see also Daniel W. Kopko, *Looking for a Crack to Break the Internet’s Back: The Listen4ever Case and Backbone Provider Liability Under the Copyright Act and the DMCA*, 8 COMP. L. REV. & TECH. J. 83, 84 (2003).

57. See Matt Hines, *RIAA Drops Amnesty Program*, CNET NEWS.COM, Apr. 20, 2004, http://news.com.com/2100-1027_3-5195301.html.

58. See, e.g., Katie Dean, *RIAA Strikes Again at Traders*, WIRED.COM, Jan. 22, 2004, <http://www.wired.com/news/digiwood/1,61989-0.html> (describing 532 newly filed lawsuits); Jen McCaffery, *Virginia Tech Computer User Is Sued By Recording Industry*, ROANOKE TIMES, Apr. 29, 2004, at A1 (describing 477 newly filed lawsuits); Nick Timiraos, *Three Students Sued By RIAA*, THE HOYA, Mar. 26, 2004, available at <http://www.thehoya.com/news/032604/news1.cfm> (describing 532 newly filed lawsuits). For a collection of the pleadings and orders in many of these cases, see <http://www.eff.org/IP/P2P/riaa-v-thepeople.php>.

The same section of the DMCA that includes the notice and takedown procedure also includes a subpoena provision designed to allow copyright owners to discover the identities of account holders who have posted infringing content on the service provider’s servers, again without judicial oversight. See 17 U.S.C. § 512(h) (2000). For reasons of statutory structure and legislative history, courts have ruled that copyright owners may not rely on this provision to discover the identities of account holders for whom the online service provider functions as a passive conduit. See *In re Charter Commc’ns, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 772 (8th Cir. 2005); *RIAA v. Verizon Internet Servs.*,

judicially-supervised subpoenas directed to the online service providers whose services were used to access the Internet; the service providers must then identify the subscribers to whom particular Internet Protocol addresses were assigned at the specified times. Both because individual defendants generally do not have deep pockets and because lengthy litigation against individuals might provoke a public backlash, the industries' preference is not to try these cases. Instead, they funnel complaints against identified users to a private settlement service center that offers them a choice between a confidential, relatively small monetary settlement and public financial ruin.⁵⁹ Most defendants quickly settle for an amount reported to be in the \$3,000–\$6,000 range.⁶⁰ Because these lawsuits typically have low filing and overhead costs, the civil settlement program has become a profit center for the industry.

Lest individuals become too blasé about the prospect of a several thousand dollar civil settlement, the civil suits are interspersed with the occasional criminal prosecution. Some prosecutions have understandable targets. For example, the U.S. Department of Justice has prosecuted several individuals who operated web sites that offered pre-release movies for download to users of the popular BitTorrent file-sharing application.⁶¹ Other targets, however, appear more randomly selected. In 2005, the recording industry convinced Arizona state authorities to prosecute an undergraduate at the University of Arizona under a state “Internet piracy” law. His conviction and sentence to a jail term followed by community service made the national wire services, and presumably came to the attention of college students across the country.⁶²

The entertainment industries also continue to experiment with attempts to interfere directly with the exchange of unprotected files by individuals on p2p networks. Technically, it is possible to use p2p networks to deliver a version of vigilante justice: “logic bombs” designed to identify and destroy unauthorized files residing on users' computers. As currently worded, however, the federal Computer Fraud and Abuse Act prohibits this conduct.⁶³ The copyright indus-

Inc., 351 F.3d 1229, 1231 (D.C. Cir. 2003), *cert. denied*, 125 S. Ct. 309 (2004). Because courts have routinely granted “John Doe” subpoena requests, the entertainment industries have not pushed Congress to rewrite § 512(h).

59. See Nick Mamatas, *Meet John Doe: The RIAA Runs Its Lawsuits as a Volume Business, and Sometimes Downloaders Just Gotta Settle*, VILLAGE VOICE, Mar. 7, 2005, <http://www.villagevoice.com/music/0510,mamatas,61813,22.html>; Andrew Tran, *Woman Silenced by Music Mafia*, DAILY TEXAN (Austin), Feb. 4, 2005, available at <http://www.dailytexanonline.com/news/2005/02/04/> (follow “Woman Silenced by Music Mafia” hyperlink).

60. See Justin Hughes, *On the Logic of Suing One's Customers and the Dilemma of Infringement-Based Business Models*, 22 CARDOZO ARTS & ENT. L.J. 725, 749 (2005). Defendants who choose trial have fared poorly. See *BMG Music v. Gonzales*, 430 F.3d 888, 891 (7th Cir. 2005) (rejecting defendant's fair use arguments and remanding for determination of statutory damages).

61. See Press Release, U.S. Dept. of Justice, Federal Law Enforcement Announces Operation D-Elite, Crackdown on P2P Piracy Network (May 25, 2005), http://www.usdoj.gov/opa/pr/2005/May/05_crm_291.htm.

62. See Beth DeFalco, *Teen Convicted Under Internet Piracy Law*, USA TODAY, Mar. 7, 2005, http://www.usatoday.com/tech/news/techpolicy/2005-03-07-az-teen-downloader-convicted_x.htm.

63. See 18 U.S.C. § 1030 (Supp. II 2002).

tries have intermittently supported legislation to create an exemption that would allow them to take the enforcement actions they desire.⁶⁴ Absent such authority, they have turned to a more benign strategy known as “spoofing”—flooding p2p networks with “decoy” files that purport to contain popular audio or video content, but that when opened contain only noise, or even warnings against copyright infringement.⁶⁵ By this campaign and their other user-directed initiatives, the entertainment industries hope to propagate a belief that p2p networks are unreliable as well as dangerous.

F. RHETORICAL POSITIONING

The sixth and final set of strategies for pervasively distributed copyright enforcement operates entirely on the rhetorical level, and seeks to mold public awareness of copyright issues. Entertainment industry representatives have deployed a variety of rhetorical tropes designed to position online copyright infringement, and particularly p2p filesharing, as morally objectionable and socially insidious. In a blizzard of press releases and media interviews, and in a variety of more formal settings ranging from conference addresses to congressional testimony, they have equated online copyright infringement with theft, piracy, communism, plague, pandemic, and terrorism.⁶⁶ In an effort both to boost demand for trusted systems functionality and shore up support for government-imposed technology mandates, they have also linked p2p filesharing with the spread of pornography and with increased risk of exposure to viruses and spyware.⁶⁷

These rhetorical initiatives have not gone uncontested. However, legal scholars and public domain advocates have tended to focus on the “theft,” “piracy,” and “communism” strands, all of which hinge on presuppositions about the extent to which copyright is really “property,” and to ignore or ridicule the other, more hyperbolic comparisons. As I will show, the rhetoric of disease and

64. See H.R. 5211, 107th Cong., 2d Sess. (2002); Ted Bridis & Lee Davidson, *Download at Your Own Risk*, DESERET MORNING NEWS (Salt Lake City), June 18, 2003, at A01 (describing statements by Sen. Orrin Hatch supporting such an approach).

65. See Sonia K. Katyal, *Privacy vs. Piracy*, 7 YALE J.L. & TECH. 222, 311–13 (2005); Jay Lyman, *P2Ps Turn Tables on RIAA, Allege Patent Infringement*, TECHNEWSWORLD.COM, Sept. 10, 2004, <http://www.technewsworld.com/story/entertainment/p2p-kazaa-altnet-riaa-36520.html>.

66. See GILLESPIE, *supra* note 4, ch. 4; Alex Cameron, *Diagnosis Technoplague: Tracing Metaphors and Their Implications in Digital Copyright* (working paper on file with author); John Logie, *A Copyright Cold War? The Polarized Rhetoric of the Peer-to-Peer Debates*, FIRST MONDAY, July 2003, http://firstmonday.org/issues/issue8_7/logie/index.html.

67. See *Content Protection in the Digital Age: The Broadcasting Flag, High-Definition Radio, and the Analog Hole: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary*, 109th Cong. 15 (2005) (statement of Mitch Bainwol, CEO, Recording Industry Association of America); *Protecting Copyright and Innovation in a Post-Grokster World: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. (2005) (statement of Ali Aydar, COO, SNOCAP); *Reducing Peer-to-Peer (P2P) Piracy on University Campuses: A Progress Update: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary*, 109th Cong. 38 (2005) (statement of Richard Taylor, Senior Vice President, Motion Picture Association of America).

terror—of crisis—plays a critical role in undergirding the other strategies. For this reason, it holds an important key to understanding the emerging phenomenon of pervasively distributed copyright enforcement as a whole.

II. NORMAL DISCIPLINE IN THE AGE OF CRISIS

Theorizing the drive toward pervasively distributed copyright enforcement has posed challenges for scholars accustomed to analyzing information markets within the framework of intellectual property law. For some intellectual property scholars, the strategies described above are simply logical responses to the economics of large-scale infringement in a networked information environment.⁶⁸ For others, they signal an efficient shift toward reliance on self-help to protect legal entitlements.⁶⁹ But the changes that these strategies portend for the networked information environment go far beyond allocative efficiency. Pervasively distributed copyright enforcement signals systemic changes in the ordering of vast sectors of activity both inside and outside markets, in response to asserted needs that are both economic and societal. Understanding these changes requires a broader range of tools than economically-inclined theorists of intellectual property rights ordinarily employ. Within social theory, important tools for theorizing the progressive deployment of pervasively distributed copyright enforcement are found in Michel Foucault's work on systems of social discipline.⁷⁰ On the whole, intellectual property scholars have read this work too narrowly, and consequently have overlooked some aspects of it that are especially relevant to understanding what the shift to pervasively distributed copyright enforcement represents.

Pervasively distributed copyright enforcement is not intended to eliminate transactions between information providers and information users, but it is intended to change the technical and legal parameters of those transactions in a way that renders them fundamentally relational on two levels. For end users, information transactions will become processes characterized by the ongoing authorization of access and use. For technology providers, transactions over technical standards will undergo a similar transformation. Relationships between information providers and information users will be mediated partly by

68. See, e.g., Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217; Hughes, *supra* note 60; Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345 (2004); Randal C. Picker, *The Digital Video Recorder: Unbundling Advertising and Content*, 71 U. CHI. L. REV. 205 (2004); see also Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395, 396 (2003) (observing that imposing liability on parties that are in a position to control infringement is efficient, but noting that other policy considerations might weigh against some extensions of indirect liability).

69. See, e.g., Douglas G. Lichtman, *Defusing DRM 9* (Univ. of Chi. Law School, John M. Olin Law & Econ. Working Paper No. 282, 2006).

70. See MICHEL FOUCAULT, *POWER/KNOWLEDGE: SELECTED INTERVIEWS AND OTHER WRITINGS 1972–1977* (1980) [hereinafter FOUCAULT, *POWER/KNOWLEDGE*]; MICHEL FOUCAULT, *DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON* (1977) [hereinafter FOUCAULT, *DISCIPLINE AND PUNISH*].

technical standards, and so pervasively distributed copyright enforcement seeks to change the ways in which these standards are developed and implemented. Usually, participation in both standards and standards development processes is determined by economic self-interest. But pervasively distributed copyright enforcement will not work properly unless compliance by licensed equipment and service providers is mandatory and verifiable. Effective implementation of pervasively distributed copyright enforcement therefore requires ongoing authorization of access to and implementation of the relevant standards.⁷¹ To understand these linked regimes of ongoing authorization as a social and historical phenomenon, intellectual property scholars must look beyond literatures about markets and standards.

Alfred Yen has suggested that the emerging web of relationships between individuals and Internet access providers resembles a quasi-feudal regime of distributed governance.⁷² Although “the Internet” as a whole cannot easily be controlled or governed, gateways to the network have virtually unlimited powers to control the parameters of access. Within this system, as in medieval systems of vassalage, “[s]tate power becomes an incident of private property that gets fragmented through delegation to numerous private parties.”⁷³ Although in theory (and *in extremis*) an Internet access provider is subject to the full extent of state authority, Yen argues that as a practical matter its authority over the day-to-day operation of its fiefdom is absolute. The comparison is an original and thought-provoking one, and it is worth considering whether it might also supply a useful way of understanding the rise of copyright enforcement and surveillance regimes.

The metaphor of the feudal fiefdom, however, seems imperfectly suited to describe the linked practices of control and ongoing authorization that characterize pervasively distributed copyright enforcement. Feudalism responded to the ungovernability of large medieval realms by partitioning geographic space into smaller and smaller parcels; likewise, the sovereignty of Internet access providers derives from their absolute authority to control traffic through and content hosted on their servers. Pervasively distributed copyright enforcement instead enables governability from afar. By insinuating automated control into formerly private spaces and activities, these technologies can obviate much of the need for localized enforcement. Pervasively distributed copyright enforcement also enables the coordination of regulation and enforcement by multiple right-

71. As Tarleton Gillespie explains, this is perhaps the most significant difference between the music industry's failed Secure Digital Music Initiative and the movie industry's successful DVD-CCA initiative. See GILLESPIE, *supra* note 4, chs. 5–6.

72. Alfred C. Yen, *Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace*, 17 BERKELEY TECH. L.J. 1207 (2002); see also Marjory S. Blumenthal & David D. Clark, *Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World*, 1 ACM TRANS. INTERNET TECH. 70, 71 (2001) (arguing that assertions of control by Internet access providers threaten the “end-to-end” principle that originally informed the design of Internet protocols).

73. Yen, *supra* note 72, at 1240.

holders, reflecting the fact that individuals may enter into a multiplicity of relationships with information providers. The disparities of power within a fully implemented set of controls are distributed and systemic; they form a network of coordinated actors, not a rigidly ordered feudal hierarchy.

Unlike the quasi-feudal regime that mediates Internet access, the emergent system of pervasively distributed copyright enforcement does not embody notions of sovereignty in the conventional (territorial, top-down) sense; instead, it infuses regulation into the artifacts and practices of daily life. The application of technology to propagate regulatory features throughout digital spaces in turn produces particular (new) configurations of those spaces, which embody new arrangements of power, and instill new expectations of conduct. To say that these developments exemplify “regulation by code” is to confuse description with explanation.⁷⁴ Understanding these developments requires a theory that encompasses the modalities of regulation by pervasive, embedded social institutions.

In search of a social theory of technology-based regulation, some cyberlaw scholars have turned to Michel Foucault’s work on the Panopticon. Devised by Jeremy Bentham, the Panopticon consisted of a central guard tower surrounded by concentric rings of cells arranged in such a fashion that the guard could see into any of them at will, but could not himself be seen. In his survey of the history of disciplinary systems, Foucault characterized the Panopticon as the perfect prison, observing that it ensured both the complete visibility of those to be surveilled and the complete invisibility of the watchers. To borrow a phrase from Jamie Boyle, for cyberlaw scholars this analogy has proved “too succulent to resist.”⁷⁵ Panoptic theories of the information age abound. In particular, privacy scholars have invoked panoptic imagery and Foucault’s discussion of Bentham to criticize the use of networked digital technologies for surveillance and profiling purposes.⁷⁶ Translating this approach to the copyright context has

74. The conventional reference is to Lessig and Reidenberg, although neither advances so simplistic a theory. See LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999) (advancing a positive theory about code as a modality of regulation and a normative theory about correspondence between digital architectures and the freedoms guaranteed in the Bill of Rights); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) (advancing a positive theory about code as a modality of regulation and a normative theory about appropriate uses of this modality by the state); see also WILLIAM J. MITCHELL, *CITY OF BITS: SPACE, PLACE, AND THE INFOBAHN* 111–12 (1995). In fact, the central insight has a much longer pedigree. See, e.g., SHAPING TECHNOLOGY/BUILDING SOCIETY: STUDIES IN SOCIOTECHNICAL CHANGE (Wiebe E. Bijker & John Law eds., 1992); LANGDON WINNER, *AUTONOMOUS TECHNOLOGY: TECHNICS-OUT-OF-CONTROL AS A THEME IN POLITICAL THOUGHT* 323 (1977).

75. James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33, 37 n.12 (2003).

76. See, e.g., OSCAR GANDY, JR., *THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION* (1993); JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* 213–14 (2000); Stan Karas, *Enhancing the Privacy Discourse: Consumer Information Gathering as Surveillance*, 7 J. TECH. L. & POL’Y 30 (2002); Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393 (2002); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 852–54 (2000); Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 864–66

proved difficult, however. The strategies of pervasively distributed copyright enforcement are not all surveillance-based. The emphasis on surveillance leads scholars to focus on some strategies while ignoring others, and paying insufficient attention to the cumulative effect of all of them.⁷⁷

This form of panoptic reasoning about the networked information age strikes some critics as a fantastic excursion into the realm of conspiracy theory. To some extent this resistance results from the implicit conflation of panoptic discipline with surveillance, but it also rests on an equation of panopticism with centralization. For scholars who make these assumptions, panoptic theories do not satisfactorily explain how the fundamentally centralized model of discipline embodied in the Panopticon translates to contexts in which neither surveillance nor control is centralized. For this reason, they conclude that while the Panopticon was an interesting and memorably named conceptual experiment, taken on its own terms it does not furnish a compelling model for many extensions of power in market-democratic societies.

As I will explain, the standard invocation of panopticism on all sides of this debate rests on an overliteral interpretation of what Foucault was about.⁷⁸ Nonetheless, there are important differences between pervasively distributed copyright enforcement and each of two distinct disciplinary models that Foucault articulated. Pervasively distributed copyright enforcement is a disciplinary hybrid, with features that merit exceptionally close consideration. Unlike either of Foucault's two real-world models, moreover, pervasively distributed copyright enforcement is panoptic discipline in exactly the Foucauldian sense.

Foucault elaborated two models of social discipline, which I will call "normal discipline" and "crisis discipline." Normal discipline encompasses the processes by which power diffuses throughout ordinary institutions and is coordinated by the everyday routines and interactions of a variety of public and private actors. Its most visible components are institutions that target marginal, abnormal, or imperfect members of society for treatment, education, socialization, or punishment. Foucault painstakingly documented and analyzed the emergence of hospitals, schools, armies, and prisons as institutions for social discipline.⁷⁹ The techniques employed consisted of the simultaneous gathering of information by surveillance and repeated examination (the observation of prisoners but also the division of schoolchildren and soldiers into ranks and the singling out of poor performers). Surveillance was enabled by partitioning geographic space—

(2002); see also Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1413–18 (2001) (exploring the limits of the panoptic metaphor).

77. See Katyal, *supra* note 65; Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297 (2004).

78. The exception is James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-wired Censors*, 66 U. CIN. L. REV. 177 (1997). Boyle persuasively refutes the notion that panoptic discipline requires the exercise of top-down sovereignty in the conventional sense. He does not address the implicit linkage of panoptic discipline with surveillance to the exclusion of other techniques.

79. See FOUCAULT, DISCIPLINE AND PUNISH, *supra* note 70, at 135–94, 231–56.

prisoners in their cells, mental patients in their wards, soldiers in their ranks, and schoolchildren in their classes. One of Foucault's central insights was that these ostensibly marginal institutions also discipline those not subject to their control, albeit indirectly.⁸⁰ Schools, hospitals, armies, and prisons normalize by exclusion; by defining, excluding, and disciplining those deemed abnormal or transitional, they simultaneously define and enforce the parameters of normalcy for everyone else.

Foucault proffered the Panopticon not as a blueprint for a particular disciplinary institution but rather as an organizing metaphor for this emergent class of "normal" disciplinary strategies, which harnessed space and visibility "to improve the exercise of power by making it lighter, more rapid, more effective, a design of subtle coercion for a society to come."⁸¹ Panoptic discipline in this metaphoric sense is not simply a function of surveillance, but also depends partly and importantly on two other factors. First, it entails an arrangement of social space that obviates the need for continual surveillance. The Panopticon was perfect in this regard because its architecture ensured continual exposure. Second and relatedly, this arrangement fosters the widespread internalization of disciplinary norms. Judged against these criteria, the institutions of normal discipline, which single out particular populations, are imperfectly coercive of the "normal" population and therefore are imperfect realizations of the idealized panoptic model.

Crisis discipline, in contrast, refers to regimes developed in response to extreme circumstances that were perceived to threaten the community's very survival. Unlike the visible mechanisms of normal discipline, those developed for crisis discipline were universally applicable. In particular, Foucault focused on the methods developed by medieval city-states for managing outbreaks of the plague.⁸² Here too, the principal tool of discipline was geographic. Although medieval physicians did not have the benefit of modern principles of microbiology and epidemiology, they understood that the plague spread by human-to-human contact. Therefore, during an outbreak, citizens were forbidden to leave their homes. Every evening, a designated corps of inspectors would go door-to-door and demand that each inhabitant of a household stand at the window to prove that he or she was still alive. If the inhabitants of a home were stricken, the home remained isolated until everyone in it had either died or shown immunity by surviving. Then, the home was scoured and its contents burned.

Considered in light of this taxonomy, many of the strategies described in Part

80. *See id.* at 210–28.

81. *Id.* at 209; *see also id.* at 205 (“[T]he Panopticon must not be understood as a dream building: it is the diagram of a mechanism of power reduced to its ideal form; its functioning, abstracted from any obstacle, resistance or friction, must be represented as a pure architectural and optical system: it is in fact a figure of political technology that may and must be detached from any specific use.”); Boyle, *supra* note 78, at 185–88 (identifying the Panopticon as the “paradigm” for a model of disciplinary power).

82. FOUCAULT, DISCIPLINE AND PUNISH, *supra* note 70, at 195–98.

I do not conform to the “panoptic” model of invisible, internalized discipline, but rather seem intended to instantiate crisis discipline. The rhetorical strategies, the pressures brought to bear on independent equipment providers and network gatekeepers, and the litigation campaign against users all are designed to signal a state of emergency. In particular, the more extreme rhetorical tropes are intended to establish that uncontrolled networked communication can spread contagion. In his decision in the DeCSS litigation, Judge Lewis Kaplan explained:

In a common source epidemic, as where members of a population contract a non-contagious disease from a poisoned well, the disease spreads only by exposure to the common source. If one eliminates the source, or closes the contaminated well, the epidemic is stopped. In a propagated outbreak epidemic, on the other hand, the disease spreads from person to person. Hence, finding the initial source of the infection accomplishes little, as the disease continues to spread even if the initial source is eliminated. For obvious reasons, then, propagated outbreak epidemics, all other things being equal, can be far more difficult to control.

This disease metaphor is helpful here. The book infringement hypothetical is analogous to a common source outbreak epidemic. Shut down the printing press (poisoned well) and one ends the infringement (the disease outbreak). The spread of means of circumventing access to copyrighted works in digital form, however, is analogous to a propagated outbreak epidemic. Finding the original source of infection (e.g., the author of DeCSS[, the computer program that decrypts the content on DVDs,] or the person to misuse it) accomplishes nothing as the disease (infringement made possible by DeCSS, the resulting availability of decrypted DVDs) may continue to spread from one person who gains access to the circumvention program or decrypted DVD to another. And each is “infected,” i.e., each is as capable of making perfect copies of the digital file containing the copyrighted work as the author of the program or the first person to use it for improper purposes.⁸³

Judge Kaplan’s elaboration of the disease metaphor for online copyright infringement is not a solitary instance of hyperbole, but rather adopts a persistent theme sounded by the copyright industries and echoed in media coverage of digital copyright issues.⁸⁴

83. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 331–32 (S.D.N.Y. 2000), *aff’d sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

84. See, e.g., *U.S. Senate Committee on Foreign Relations Holds Hearing on Evaluating International Intellectual Property Piracy*, in FDCH POLITICAL TRANSCRIPTS, June 9, 2004 (statement of Jack Valenti, President and CEO of the Motion Picture Association of America), available at 2004 WL 1294332; Suzanne Choney, *Piracy Keeps Online Music From Singing a Happy Tune*, SAN DIEGO UNION TRIB., May 3, 2004, at C1; James Flanigan, *Asset-Heavy Companies Need to Slim Down*, L.A. TIMES, Jan. 19, 2003, at C1; *Strategies to Sink the Music Pirates*, THE AUSTRALIAN, July 18, 2003, at 10; Tom Zucco, *Unchained Melodies*, ST. PETERSBURG TIMES, Sept. 30, 2002, at D1; Cameron, *supra* note 66 (collecting uses of the plague metaphor); Olga Kharif, *Facing the Digital Music at Record Shops*,

Extraordinary threats demand extraordinary countermeasures. If online copyright infringement is the plague, and direct, unmediated human-to-human communication is its medium of transmission, then we might expect proposals for extreme restrictions on communication to follow. As Foucault explains, one responds to a great threat that travels by human contact in the only way possible—by eliminating contact:

[A]gainst an extraordinary evil, power is mobilized; it makes itself everywhere present and visible; it invents new mechanisms; it separates, it immobilizes, it partitions; it constructs for a time what is both a counter-city and the perfect society; it imposes an ideal functioning, but one that is reduced, in the final analysis, like the evil that it combats, to a simple dualism of life and death: that which moves brings death, and one kills that which moves.⁸⁵

The phenomenon of online copyright infringement differs from a microbial epidemic in one important way that affects the selection of countermeasures. The germs that cause bubonic plague have no positive qualities, and there is no independent reason to disseminate them. Copyrighted content, in contrast, must be disseminated broadly in order for its producers to earn a profit. The deadly vector is not the protected work, but the unprotected work. The “propagated outbreak epidemic” to which Judge Kaplan referred is simply an example of a more general property of networks of all sorts;⁸⁶ the content industries are not averse to harnessing the considerable benefits of network distribution for their own purposes. An effective disciplinary regime therefore must concentrate on preventing users from converting protected to unprotected content.

The strategies for control described above are intended to accomplish precisely this separation of protected from unprotected content. The techniques of ongoing authorization, automated enforcement, and widely distributed policing obligations adapt the philosophy and instrumentalities of plague control to the digital age. More precise control of interactions with information goods obviates the need for physical confinement of persons, while direct functionality restrictions and trusted systems protocols serve to ensure that protected information carries the terms of its confinement with it.

Upon closer consideration, however, pervasively distributed copyright enforcement does not precisely fit the crisis discipline model, either. Crisis discipline is temporary and highly visible, while pervasively distributed copyright enforcement is intended to be permanent, and to become gradually more invisible as patterns of user behavior evolve. If the technology-based strategies described in

BUSINESSWEEK ONLINE, June 21, 2001, http://www.businessweek.com/technology/content/jun2001/tc20010621_232.htm; Richard Shim, *News Corp. Exec Puts Piracy in the Spotlight*, CNET NEWS.COM, Nov. 19, 2002, <http://news.com.com/2100-1040-966457.html>.

85. FOUCAULT, DISCIPLINE AND PUNISH, *supra* note 70, at 205.

86. For a concise, highly readable explanation, see ALBERT-LASZLO BARABASI, LINKED: THE NEW SCIENCE OF NETWORKS 123–42 (2002).

Part I work as intended, the underlying regime of protocols, authorizations, and other gatekeeping mechanisms will simply fade into the background. This raises the question whether the current struggles simply mark a moment of transition to a new regime of normal discipline. In the longer term, perhaps it is a mistake to regard the shift to pervasively distributed copyright enforcement as anything more than a shift in norms. Yet the emergent model of pervasively distributed copyright enforcement has important features that the regimes of normal discipline outlined by Foucault did not. The shift to pervasively distributed copyright enforcement signals the emergence of an anomalous, hybrid form of discipline predicated on permanent crisis.

Consider again the distinctive attributes of each mode of discipline that Foucault described: Crisis discipline is centralized, universal, and highly visible, but temporary. Normal discipline is the polar opposite: It is decentralized, differential, and largely invisible, but permanent. Pervasively distributed copyright enforcement does not align perfectly with either model. Like crisis discipline, it is (or aspires to be) universally restrictive; like normal discipline, it is intended to be permanent. Its constituent strategies are not centralized and visible, but neither are they wholly decentralized and wholly invisible. Pervasively distributed copyright enforcement is a mode of managing an ongoing crisis that cannot be completely resolved. Crisis management consists in the establishment and normalization of coordinated patterns of authorization and constraint.

Let us begin with permanency. Foucault's model of crisis discipline does not encompass conditions of permanent emergency. In the societies that originated the techniques of plague control, emergencies were temporary. As the plague passed, so did the ability to sustain the extreme measures it was thought to justify. Medieval burghers were not placed under house arrest indefinitely, but only until the plague had been isolated and purged from each place it had touched. The implicit definition of acute danger as episodic does not translate well to the context of online copyright infringement. Here again, Judge Kaplan's reasoning is illustrative:

The disease metaphor breaks down principally at the final point. Individuals infected with a real disease become sick, usually are driven by obvious self-interest to seek medical attention, and are cured of the disease if medical science is capable of doing so. Individuals infected with the "disease" of capability of circumventing measures controlling access to copyrighted works in digital form, however, do not suffer from having that ability. They cannot be relied upon to identify themselves to those seeking to control the "disease." And their self-interest will motivate some to misuse the capability, a misuse that, in practical terms, often will be untraceable.⁸⁷

What happens to disciplinary modalities when crisis is not temporary, but a permanent state of affairs? As Foucault's work on normal discipline suggests, a

87. *Reimerdes*, 111 F. Supp. 2d at 332.

hallmark of (modern) times of relative normalcy is that more subtle, less direct modes of discipline come to the fore. The institutions of normal discipline take the form of “a generalizable model of functioning; a way of defining power relations in terms of the everyday life of men.”⁸⁸ These disciplinary methods work, in other words, because citizens of a society internalize the criteria that they apply. Normal discipline labels and smooths away quotidian challenges to the fabric of social life. We carry our conditioning, and our blinders, with us.

If the sense of continuing crisis articulated by Judge Kaplan is sufficiently widespread—and the rhetorical strategies of pervasively distributed copyright enforcement are crafted to convince us that it is—then, using Foucault’s observations as a guide, we might expect to see a hybrid form of discipline coming into existence. This hybrid regime would require a generalizable model of functioning, sustainable on a day to day basis. The model would condition both by direct behavioral restrictions and by the more subtle mechanisms of normalization. It would also retain the capability to respond with appropriate severity to the conditions that brought about the crisis in the first place. Pervasively distributed copyright enforcement meets all of these requirements. It is predicated on technical and legal strategies for separating protected from unprotected content—for operationalizing plague control—but also and importantly for normalizing the processes and technologies that accomplish the separation. Fundamental to pervasively distributed copyright enforcement is the capacity to “kill that which moves” on the justification that the state of emergency is always with us.

A hybrid disciplinary model need not entail theoretical or practical inconsistencies. The crisis discipline of plague control was not sustainable for long periods of time because of the massive expenditure of resources it entailed and the near-complete suspension of ordinary activity that it required. It does not follow, however, that all methods of crisis control are equally maladapted for long-term use. Here it is useful to reconsider the prison (in its real-world form, not the idealized Panopticon) as a model for both perpetuation and containment of a form of crisis discipline within the larger social framework. Societies isolate prisoners to avert crisis, and the enterprise of prison-maintenance need not entail a total breakdown of “normal” social functioning; indeed, Foucault’s account suggests that prisons serve partly to enable such functioning. Prisons operate by geographic containment of people, but the point is a more general one: Normal discipline and crisis discipline are not mutually exclusive chronological states, and their boundaries will constantly be subject to (re)negotiation.⁸⁹

88. FOUCAULT, DISCIPLINE AND PUNISH, *supra* note 70, at 205.

89. For perceptive discussions of this problem in the more traditional context of threats to national and domestic security, see Bruce Ackerman, *The Emergency Constitution*, 113 YALE L.J. 1029 (2004); Oren Gross, *Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?*, 112 YALE L.J. 1011 (2003). Gross, in particular, argues that the assumption of temporal and geographic separation between normal and crisis conditions is fatally undermined by the realities of modern geopolitics, and that “[w]ithout separation, it is but a short step to conflate emergency powers and norms with the

The example of the prison, though, raises interlinked questions of universality and legitimacy. Prisons undergird a regime of normal discipline that weighs least heavily on the normal; that is both its point and its method. Pervasively distributed copyright enforcement does not fit this pattern. Its most severe restrictions are designed to bind everyone, and indeed could not be implemented differentially. In this respect they are more like plague control measures, but plague control was temporary. The shift to pervasively distributed copyright enforcement thus holds the potential to accomplish a breathtakingly inclusive extension of control, of the type that Foucault's medieval rulers might have wished, but did not dare, to put in place. Whether this is feasible depends in part on public perceptions of the conditions asserted to constitute a crisis; the rhetorical strategies of pervasively distributed copyright enforcement are directed principally toward this end. But Foucault's work on normal discipline should remind us that the success of a permanent disciplinary regime does not depend on its ability to foster constant awareness of danger. The legitimacy of permanent, universal restrictions depends importantly on their perceived obtrusiveness. Normal discipline succeeds most completely when we stop noticing that it is there.

A hallmark of normal discipline is the seamless integration of disciplinary mechanisms within the fabric of everyday life, and so pervasively distributed copyright enforcement aims for just this sort of seamless integration. Each of the six strategies is a means of instilling in consumers and technology providers an unquestioning acceptance of both the particular boundaries, and a particular overarching conception of boundedness, that content owners want. Yet pervasively distributed copyright enforcement does not seek to instill acceptance by the "normal" population principally through the articulation and internalization of norms. Containing crisis also entails establishing technical and market path-dependencies that themselves come to be seen as normal and natural. The strategies of pervasively distributed copyright enforcement redraw the boundaries of private discretion to determine the rules of interaction with content. Rather than normalizing those who remain on the "right" side of the new boundaries, it seeks to normalize a regime of universal, technologically-encoded constraint.

The resulting regime of crisis management is neither wholly centralized nor wholly decentralized; it relies, instead, on coordination of technologies and processes for authorizing information flows. Alexander Galloway has argued that the constraint effectuated by technical protocols is not a continuation of "discipline" in the sense described by Foucault but a new mode of social

'ordinary' and the 'normal.'" Gross, *supra*, at 1069–96. Ackerman concurs, but believes that the extent to which crisis mentality becomes normalized will depend substantially on how "emergency" is understood. Ackerman, *supra*, at 1039–45. As the remainder of this essay will suggest, I believe both are right.

ordering in its own right.⁹⁰ At least as applied to pervasively distributed copyright enforcement, however, that argument reifies the technical at the expense of the social. Particular forms of protocol do not evolve by happenstance, and the ways in which they evolve are important to understanding the social orderings that they support. Protocol does not supersede or substitute for discipline, but amplifies it.

The hybrid discipline of pervasively distributed copyright enforcement is panoptic discipline in exactly the Foucauldian sense: It is a coordinated set of architectural and behavioral constraints the primary function of which is not to enable surveillance but instead to obviate the need for it. It is intended to produce internalization of the “correct” rules for interacting with digital content, but it also is broadly coercive in a way that a primarily norm-based regime is not. To characterize pervasively distributed copyright enforcement simply as “the new normal,” as some of its proponents have suggested, is to mistake its magnitude and fundamentally misapprehend its operation. Evaluating pervasively distributed copyright enforcement requires a more careful, critical approach, and one that considers all of its constituent strategies.

III. CRISIS MANAGEMENT AND MARKET ORDERING

For two distinct groups of critics, the rubric of coercion that animates Foucauldian theory, and that underlies my account of pervasively distributed copyright enforcement as crisis management, is not a compelling one. Critics in the first group, whom I will call market libertarians, argue that in a decentralized market economy, whatever modes of social ordering emerge from the market will be modes that are chosen by market participants, including information vendors, technology vendors, and information consumers. Arguably, it is a mistake to regard discipline imposed in this fashion as anything other than voluntary, and if it is voluntary it is a waste of time to worry about whether it is coercive in a more abstract, theoretical sense. Critics in the second group, whom I will call speech libertarians, agree that the decentralized, loosely coordinated strategies of pervasively distributed copyright enforcement evidence coercive intent, but argue that individual liberty will prove impervious to control. In particular, they point to the continued existence of thriving darknets as evidence that pervasively distributed copyright enforcement cannot succeed. The speech libertarian objection is the subject of Part IV; here, I consider the market libertarian objection. What counts as coercion within social theory and what counts within legal theory need not be identical. Even so, pervasively distributed copyright enforcement forces choices that market participants otherwise might not be inclined to make.

How, exactly, does the emerging phenomenon of pervasively distributed

90. ALEXANDER R. GALLOWAY, *PROTOCOL: HOW CONTROL EXISTS AFTER DECENTRALIZATION* 20–27 (2004).

copyright enforcement acquire the authority to subject practices of intellectual consumption to the instrumentalities of plague control? Like Bentham's model of the Panopticon, Foucault's paradigm case of crisis discipline involved deployment by a centralized and highly authoritarian government. Under those circumstances, the power to implement crisis control measures may safely be presumed. The technology-based strategies described in Part I are for the most part deployed and coordinated by a decentralized network of private actors. Still missing from the account of these initiatives as crisis management is an explanation of the logic that underlies their privatization and decentralization.

Answering this question requires, first, some consideration of the origins of power, a problem in which Foucault himself seemed relatively uninterested.⁹¹ Although discipline is rooted in power, Foucault was less concerned with tracing power back to its roots than with mapping its imprint in the processes of everyday life. The two problems, however, are linked. This is perhaps clearest in the case of normal discipline. Any modern society will have schools, prisons, armies, and hospitals, but the methods practiced within these institutions will vary from society to society based on other institutions and ideologies. The working out of power through institutional mechanisms proceeds by way of a complex set of mutually constituting relationships. Yet this proposition also holds true for mechanisms of crisis discipline. In all but the most authoritarian societies, disciplinary mechanisms must negotiate interrelated issues of feasibility and legitimacy. In crisis, this negotiation becomes easier, but not infinitely so.

Anthony Giddens's theory of power as structuration is particularly useful for understanding the elaboration of power within a decentralized network of public and private actors.⁹² Giddens substitutes a robust vision of human agency for the "docile bodies" of Foucauldian social theory; he argues that individuals and groups are not simply the passive products of larger social forces, but make self-aware and self-interested decisions. At the same time, the theory's central premise is that human interactions are constrained, though not determined, by the "resources" of each group of actors and by each group's own habitual, or "recursive," practices.⁹³ The tension between self-interested action and the constraints of authority and practice drives the evolution of human institutions, which proceeds in pathways that are simultaneously predictable and contingent.

91. See, e.g., FOUCAULT, *POWER/KNOWLEDGE*, *supra* note 70, at 104–08; Michel Foucault, *Afterword: The Subject and Power*, in HUBERT DREYFUS & PAUL RABINOW, MICHEL FOUCAULT: BEYOND STRUCTURALISM AND HERMENEUTICS 208, 221 (1982).

92. ANTHONY GIDDENS, *THE CONSTITUTION OF SOCIETY: OUTLINE OF THE THEORY OF STRUCTURATION* (1984).

93. See *id.* at 2–28; cf. PIERRE BOURDIEU, *PRACTICAL REASON: ON THE THEORY OF ACTION* 31–34 (1998) (characterizing "social space" as the dynamic product of interactions between "agents . . . with differentiated means and ends according to their position in the structure of the field of forces, thus contributing to conserving or transforming its structure"); PIERRE BOURDIEU, *OUTLINE OF A THEORY OF PRACTICE* (1977) (developing a theory of social practice as consisting of purposive pursuit of "strategies" rather than automatic adherence to "rules").

Viewed through the lens of structuration theory, the drive toward pervasively distributed copyright enforcement may be understood as flowing from the self-interested interactions of a number of relevant groups.

The perceived need to control the threat of online copyright infringement supplies both information providers and governments with powerful (though slightly different) motives for the pervasive extension of control. Information providers seek, first and foremost, to enforce what they perceive as “their” entitlements. Because intellectual property entitlements are limited rights, this characterization involves considerable oversimplification and a certain amount of overreaching. At the same time, though, one must acknowledge this overreaching as an attempt to avert what is perceived, rightly or not, as a catastrophic threat to business models heavily dependent on the limitations of analog technologies. This response may be shortsighted, but it is entirely understandable. Arguments that the business models now dominant in the content industries should succumb to a whirlwind of Schumpeterian creative destruction, while appealing to academic commentators, hold much less appeal for those on the receiving end of the whirlwind.⁹⁴ Under the circumstances, it is not surprising to find information providers resorting to their time-tested repertoire of recursive practices—licensing, litigation, lobbying, and public relations—to preserve the market positions to which they have grown accustomed.

Government motives to support the extension of surveillance and control by private information providers are more complex. Governments are in general sympathetic to the asserted need to protect private property, both for idealistic reasons related to notions of the social contract and the rule of law and for less idealistic reasons related to legislative and regulatory capture and the promotion of trade-related agendas. Thus one might logically expect to see extensive state backing of private intellectual property enforcement efforts undertaken by powerful domestic industries, and in fact this has been the case.

Given this confluence of private and state interests, what is interesting is the extent to which mechanisms for control and surveillance of information use are envisioned as operating independently of direct government involvement. The anti-circumvention and anti-device provisions of the DMCA operate primarily as a backstop for the direct regulation to be effectuated by “trusted systems” technologies, and the notice-and-takedown provisions applicable to Internet service providers deliberately shift government out of the picture.⁹⁵ The proposed technology mandates described in Part I have been crafted to function primarily as mechanisms for coordinating industry-driven standards development and licensing processes.

Here it is important to understand that the emerging network of private disciplinary measures serves both private and state interests far better than more

94. See, e.g., Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263 (2002).

95. See 17 U.S.C. §§ 512, 1201(a)–(b) (2000).

extensive official involvement might.⁹⁶ To the extent that pervasively distributed copyright enforcement remains primarily a matter of industry initiative, information providers enjoy virtually complete freedom to define the scope of their entitlements.⁹⁷ From the perspective of the state, meanwhile, the installation of technologies that generate detailed records of information use also serves other state interests, including censorship and the containment of terrorism.⁹⁸ Precisely for this reason, however, devolution of enforcement power into private hands is essential. Generally speaking, in democratic societies, government surveillance initiatives incur far more searching public scrutiny and meet with far more resistance than analogous private efforts deployed to enforce private bargains. To take just a few examples, the U.S. government's controversial Total Information Awareness initiative, an attempt to implement comprehensive "dataveillance" of U.S. citizens, residents, and visitors, quickly became mired in congressional hearings.⁹⁹ The CAPPs II airline passenger profiling initiative fared slightly better, in part because it was (or at least appeared to be) more narrowly targeted, but ultimately succumbed in the face of intense pressure brought to bear on it by critics and open government watchdogs.¹⁰⁰ The next such initiative, the Secure Flight program, met the same fate.¹⁰¹ The USA PATRIOT Act, which conferred expanded surveillance powers on federal authorities in the wake of the September 11, 2001, terrorist acts, has been mired in controversy since its enactment. Except among a small group of technological and legal cognoscenti, private-sector trusted systems initiatives have generated comparatively few ripples of alarm.

Deploying crisis management through the marketplace remains, nonetheless, a somewhat trickier business than deploying it by state fiat. A satisfactory

96. Cf. Boyle, *supra* note 78 (arguing that states need not employ conventional, top-down regulation to gain regulatory leverage).

97. Niva Elkin-Koren has aptly characterized the resulting entitlements as "rights without laws." Niva Elkin-Koren, *Copyrights in Cyberspace—Rights Without Laws?*, 73 CHI.-KENT L. REV. 1155 (1999).

98. See Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6 (2003).

99. See *Senate Rebuffs Domestic Spy Plan*, WIRED.COM, Jan. 23, 2003, <http://www.wired.com/news/politics/0,1283,57386,00.html>. For an insightful discussion of the factors that influence both the level of public outrage and the success of public protests directed at technical developments that threaten privacy, see LAURA J. GURAK, PERSUASION AND PRIVACY IN CYBERSPACE: THE ONLINE PROTESTS OVER LOTUS MARKETPLACE AND THE CLIPPER CHIP (1997).

100. See U.S. GEN. ACCOUNTING OFFICE, GAO-04-385, AVIATION SECURITY: COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM FACES SIGNIFICANT IMPLEMENTATION CHALLENGES (2004); Sara Kehaulani Goo & Robert O'Harrow, Jr., *New Airline Screening System Postponed; Controversy Over Privacy Leads to CAPPs II Paring, Delay Until After Election*, WASH. POST, July 16, 2004, at A2; Jon Marino, *Fixes Promised For Planned Airport Screening System*, L.A. TIMES, Feb. 13, 2004, at A38; Alexandra Marks, *Big Business Joins Fight Against New Airport Screening*, CHRISTIAN SCI. MONITOR, Feb. 12, 2004, at 3; Mary Lou Pickel, *TSA Data Assertion Disputed by Delta*, ATLANTA J.-CONST., June 24, 2004, at 1D.

101. See U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-06-374T, AVIATION SECURITY: SIGNIFICANT MANAGEMENT CHALLENGES MAY ADVERSELY AFFECT IMPLEMENTATION OF THE TRANSPORTATION SECURITY ADMINISTRATION'S SECURE FLIGHT PROGRAM (2006); SECURE FLIGHT WORKING GROUP, REPORT OF THE SECURE FLIGHT WORKING GROUP (2005), http://www.epic.org/privacy/airtravel/sfwg_report_091905.pdf; Elec. Privacy Info. Ctr., *Secure Flight*, <http://www.epic.org/privacy/airtravel/secureflight.html> (last visited May 4, 2006).

explanation of the logic of pervasively distributed copyright enforcement must take into account the motives, resources, and recursive practices of several additional groups of actors.¹⁰² Of these, the ultimate users of information goods are by no means the most important.

The “market for technological protection” is, in the first instance, not the end-user market for digital content but rather the market of intermediary licensors, which includes both content distributors and manufacturers of devices for rendering the content. Within this market, the longer-term goal of pervasively distributed copyright enforcement is not so much to eliminate third-party independents as simply to eliminate their technological independence by recruiting them into the contractual networks that implement surface-level technological restrictions and trusted systems protocols. The twin threats of indirect infringement liability and DMCA liability supply additional incentives to join these networks. Although users have repeatedly shown that they will reward entrepreneurs who provide them with freedom and flexibility to use, manipulate, copy, and redistribute digital content, the costs of providing freedom have risen sharply in the wake of the content industries’ highly-publicized legal victories against MP3.com, Napster, Grokster, SonicBlue, and other innovators. The costs of raising startup capital have risen commensurately, and may become prohibitive if the suit against Napster’s backers succeeds. Increasingly, therefore, the rational strategy is to license content and build devices subject to restrictions, regardless of whether the intermediary might otherwise prefer a different strategy.

Large incumbents in the consumer electronics and personal computing markets have greater resources and face less extreme risks, and have successfully resisted some copyright industry initiatives to impose broadly defined mandates that would disrupt existing markets and distribution systems. They have been much less inclined to resist the incremental introduction of surface-level restrictions in newer technologies, such as DVD players, digital music and video game players, and software-based multimedia devices. And, as discussed in Part I, they have participated in efforts to develop trusted systems functionality for digital media files and digital broadcast content. In part this behavior reflects simple self-interest; a large consumer electronics manufacturer must, if it wishes to maintain market share, manufacture DVD players capable of playing commercially-released DVDs. Some firms in this category, such as Sony, are also content providers or affiliated with content providers; for these firms, the calculus of costs and benefits is even more complex and depends on the relative power and profitability of the affected business units. In part, however, consumer electronics manufacturers’ very different responses to different technology-based initiatives reflect the fact that consumer expectations regarding new methods of distributing and rendering multimedia content are less fully formed.

102. The remainder of this section extends and deepens the preliminary analysis sketched in Julie E. Cohen, *DRM and Privacy*, 18 *BERKELEY TECH. L.J.* 575, 614–15 (2003).

Acquiescing to content industry demands regarding copy-protection for DVD-based movies did not carry the same level of perceived marketplace risk as it does for CD-based music or free broadcast television.

Large Internet service providers confront an equally complex calculus. Many of these providers initially resisted content industry demands for identification of individual subscribers accused of engaging in p2p file-sharing.¹⁰³ But the large telephone and cable companies that provide most residential Internet access also have other agendas of their own. Many of these companies seek to use their newly-installed, high-speed fiber-optic networks to establish quality of service pricing, and to deliver their own proprietary content to subscribers.¹⁰⁴ Therefore, they are not generally averse to technologies for flagging and sorting network traffic. Cable companies also have participated in the ongoing effort to develop a regulatory framework establishing trusted systems protection for cable television content.¹⁰⁵

The interplay of supply and demand in the market for technological protection is further complicated by the dynamics of technical standardization. Because most copyright owners lack the technical expertise to build TPMs or trusted systems technologies for themselves, they must hire others to do it for them. Technology companies and researchers therefore play pivotal roles in the development and extension of pervasively distributed copyright enforcement.

Technologies, like other artifacts, are designed with particular specifications in mind; thus, technology companies do not seek simply to build the “best” system, but rather to build the best system for a given purpose or set of purposes.¹⁰⁶ As in any other market, those purposes are determined at least in part by the customer, and here again it is incorrect to assume that the most relevant customer is the end user. In the case of technological standards that mediate interactions with copyrighted content, it is increasingly the large content industries, and to some extent lawmakers, that developers must first aim to please. Within the fledgling “digital rights management” industry, vendors compete vigorously with one another to win the content industries’ business. Members of this industry also have learned to press their interests before legislators with increasing sophistication. Unaffiliated and academic researchers have been more inclined to cast a critical eye on these processes.¹⁰⁷ Perhaps

103. See *supra* note 58.

104. For discussion of these initiatives, see Susan P. Crawford, *Network Rules*, 70 *LAW & CONTEMP. PROBS.* (forthcoming 2007).

105. See Commercial Availability of Navigation Devices and Compatibility Between Cable Systems and Consumer Electronics Equipment, 68 Fed. Reg. 66,728 (Nov. 28, 2003) (to be codified at 47 C.F.R. pts. 15, 76).

106. Cf. DONALD MACKENZIE, *KNOWING MACHINES: ESSAYS ON TECHNICAL CHANGE* 54–63 (1996) (arguing against the belief that technological developments have fixed trajectories that are innately determined); WINNER, *supra* note 74 (arguing that “technology” is not an autonomous force, but rather politics by other means); Steve Woolgar, *Configuring the User*, in *A SOCIOLOGY OF MONSTERS: ESSAYS ON POWER, TECHNOLOGY AND DOMINATION* 57 (John Law ed. 1991).

107. See, e.g., Freedom to Tinker, <http://www.freedom-to-tinker.com>.

even more than their colleagues at for-profit companies, however, these individuals are highly motivated to solve the difficult theoretical problems that instantiation of this functionality requires.¹⁰⁸

For developers of trusted systems functionality, the mix of incentives, strategies, and habitual practice is even more complicated. In particular, developers of computer operating systems and microprocessors must satisfy many groups of customers. As already noted, some developers, including most notably market leaders Microsoft and Intel, appear to believe that trusted systems capabilities mesh well with other design goals, such as enhanced network, server, and file security. For Microsoft in particular, deployment of this functionality also seems bound up with a number of other business-related objectives, including protection of its proprietary technical information and preservation of its market position vis-à-vis open source software.¹⁰⁹ Other technical developers are less certain about the benefits of trusted systems functionality, but seek to avoid “technology mandates” from the government, and appear to perceive voluntary development efforts as the lesser of two evils. It is worth noting, finally, that “technology mandates” can take many forms. The government is also an important customer for trusted systems technologies, which it sees as serving other security-related goals.¹¹⁰

The choices and practices of content intermediaries and standards developers do not prevent end users from resisting functionality that they find undesirable or offensive, but they make resistance more difficult and therefore less likely. Within the market for protected content, user resistance might manifest either as refusal to buy or as refusal to submit to the discipline of the technology. As discussed in Part I, early versions of surface-level technological protection have provoked both kinds of user pushback. At higher levels of penetration, however, both kinds of market resistance become more difficult. The more deeply embedded trusted systems functionality becomes, the harder it will be to avoid by purchasing noncompliant or alternative equipment. Particularly as more and more desired features and services are bundled with this functionality, the costs of opting out may rapidly come to outweigh the benefits.¹¹¹ For all but a small group of technically skilled end users, more deeply embedded controls also are much harder to evade by circumvention.

108. See, e.g., PROCEEDINGS OF THE 5TH ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT (2005); PROCEEDINGS OF THE 4TH ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT (2004); PROCEEDINGS OF THE 3RD ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT (2003). All of these collections are available via http://portal.acm.org/browse_dl.cfm?linked=1&part=series&idx=SERIES11158&coll=ACM&dl=ACM&CFID=72913374&CFTOKEN=59431387. Cf. Bourdieu, *supra* note 93, at 138–39 (“The scientific field, this scholastic universe where the most brutal constraints of the ordinary social world are bracketed, is the locus of the genesis of a new form of necessity . . . in it the logical constraints . . . take the form of social constraints (and vice versa).”).

109. See, e.g., Microsoft Corp., *Shared Source Initiative: Open Source Software* (Feb. 1, 2004), <http://www.microsoft.com/resources/sharedsource/Government/opensource.mspx>.

110. For discussion of the emerging “security-industrial complex,” see ROBERT O’HARROW, JR., NO PLACE TO HIDE (2005).

111. See also Zittrain, *supra* note 49 (arguing that many consumers will choose to run only trusted applications and files because they fear malware attacks).

At higher levels of trusted systems penetration, moreover, open source software may no longer provide a viable alternative for individuals who want lawful, “normal” access to mainstream media content. There are already some formidable institutional obstacles to the development of open source media players that incorporate the required technological protection functionality. I have noted that industry-sanctioned standards are licensed as trade secrets, under conditions that forbid licensees from altering or disclosing information about how they work. Because both disclosure and unrestricted evolution are central tenets of open source philosophy and practice, open source developers are unlikely to accept these restrictions, and devices incorporating the restrictions will not qualify as open source products.¹¹² Reverse engineering to develop unlicensed open source media players most likely violates the DMCA. The statutory exception for reverse engineering does not shelter efforts to achieve format interoperability for digital content that is not itself a computer program; in any case, that exception also forbids widespread sharing of the information gained from reverse engineering.¹¹³

In theory, more meaningful possibilities for end-user resistance might arise in the market for standards, at the point where policy is inscribed in technology. Here, though, users must be determined enough and informed enough to overcome a series of significant hurdles, including the relative opacity of computing infrastructures, the need to understand and appreciate the significance of automated enforcement measures long before implementations surface in the consumer marketplace, the closed nature of many standard-setting processes, and the technical complexity of the subject matter.¹¹⁴ Some consumer advocacy groups have begun to do exactly this; what remains to be seen is whether these efforts will generate enough critical mass to affect the content of technological protection standards.

Finally, the ideology of the marketplace itself reinforces the extension of pervasively distributed copyright enforcement, in two distinct and opposite ways. The first involves the mirror image of the argument about motives for privatization made above: Just as privatization legitimates self-enforcing authorization and constraint, so privatized authorization and constraint reinforce the

112. This perhaps explains the fact that although the DVD-CCA has issued several licenses to develop open-source DVD players that incorporate CSS decryption capability, and trumpeted this fact in the DeCSS litigation, no DVD player that is both fully open-source and capable of installation on a Linux operating system has actually been developed. See Keith J. Winstein, *Real Dialogue: The Tech Interviews Jack Valenti*, THE TECH, Apr. 16, 2004, <http://www-tech.mit.edu/V124/N20/ValentiInterviewe.20f.html>. For discussion of the divergence between open source methodologies and the trusted systems approach, see GILLESPIE, *supra* note 4, ch. 8.

113. See 17 U.S.C. § 1201(f) (2000); *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 319 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

114. Cf. GURAK, *supra* note 99, at 66–83 (describing how the technical complexity of the issues surrounding deployment of the Clipper Chip created obstacles to the generation of a popular protest movement).

perception that the discipline imposed is freely chosen by arms-length contracting parties. Second, to the extent that industry enforcement and public education efforts fuel popular resistance to pervasively distributed copyright enforcement, increased popular resistance in turn fuels and legitimates the rhetoric of crisis and the extension of technologies to control it. Any ratcheting up of crisis mentality increases the downside risks of contributory infringement liability for independent entrepreneurs and government oversight for standards developers. In short, even as pervasively distributed copyright enforcement fails to convince end users, it strengthens its hold on the intermediaries whose products, services, and standards define the end-user marketplace.

For all of these reasons, we might predict both that pervasively distributed copyright enforcement must be privatized and decentralized to be effective, and that at least some such initiatives might well succeed. Once again, it is important to note that this analysis is provisional and speculative; it remains possible that the nascent relationships of power, authority, and acquiescence could be disrupted in important ways. The point simply is that the dynamics of marketplace acceptance and rejection are complicated, and that choices available in markets are not inconsistent with, and may enable, the imposition of highly restrictive disciplinary regimes that many market participants experience as onerous—regimes justified by crisis and internalized as obligation. In important and mutually reinforcing ways, the recursive practices of market actors lend authority to the linked strategies of crisis management.

IV. CRISIS MANAGEMENT AND THE PRODUCTION OF NETWORKED SPACE

Thus far, I have simply attempted to describe the emerging social phenomenon of pervasively distributed copyright enforcement and locate it within a rough taxonomy of disciplinary practices, without questioning either the logic of the disease metaphor as applied to online copyright infringement or the efficacy of the proposed cure. It is time to take stock. How should we think about the discipline that this vision, if brought to fruition, would inculcate? Here it is important to consider the speech libertarian objection very carefully. Perhaps the sort of control that pervasively distributed copyright enforcement seeks to instantiate simply cannot be achieved. Perhaps, then, pervasively distributed copyright enforcement simply will not matter very much. The first conclusion is probably right, but the second does not follow.

Evaluating pervasively distributed copyright enforcement requires careful consideration of both its benefits and the other changes that normalization of this particular form of crisis discipline is likely to produce. The analysis must begin by acknowledging that the opposite of “discipline” is not freedom, but anarchy. The terms “society” and “civilization” necessarily presuppose functioning disciplinary mechanisms: institutions that apply (and act upon) shared values to mediate and structure human interaction. To all except the most dedicated pessimist, the ubiquity of discipline is a good thing, not a bad thing; it is what enables collective political, social, and economic enterprise. The larger

question, then, is not “whether discipline?” but “what discipline?” In particular, we must consider whether normalization of crisis management would serve a broader range of productive interests, and whether it would further or frustrate important noninstrumental values.

To the extent that pervasively distributed copyright enforcement enables detection, punishment, and/or prevention of large-scale copyright infringements, it will produce some clear benefits. These benefits, moreover, are not exclusively private; society as a whole derives important benefits from a stable system of intellectual property protection. Within both markets and firms, intellectual property rights facilitate the productive organization of economic activity, with a variety of attendant welfare gains. Persistent and important distributional objections to this activity should not cause us to overlook the considerable good it also generates. Society as a whole also derives benefits from the productive resolution of crisis, and more particularly from the working out of strategies for adapting sustainably to technological change.

The extent of both benefits, however, is open to considerable debate. Many argue that a system of intellectual property protection produces the greatest social gain when rules granting protection are balanced by offsetting limits. One can acknowledge the benefits of clear intellectual property entitlements while still reserving rather substantial questions about how much protection and how much enforcement are optimal. Similarly, some resolutions of crisis are more productive than others. The first problem has been analyzed exhaustively elsewhere; here, I will focus on the second. Let us consider now some additional entailments of the normalization of this particular mode of discipline.

The shift to crisis management is intended first and foremost to affect the ways in which individual users of information goods experience flows of information; thus, it is important to begin by asking how individuals experience information and what they use it for. Discussions of these questions within the legal literature have tended to assume a set of disembodied, purposive interactions. This model does not lend itself well to understanding what the shift to pervasively distributed copyright enforcement represents. Research in human cognition suggests that reasoning and perception are embodied: We perceive features of our immediate environment through and in relation to the embodied, situated self, and formulate physical and spatial metaphors to convey abstract concepts.¹¹⁵ The list of metaphors commonly used to describe information-related activities, both online and off, bears out these conclusions. On the network we surf, visit sites and domains, download files, and post messages; within our private computing environments we consume cultural products, absorb and digest facts and opinions, advance arguments, and rip, mix, and burn sounds and images. From the individual perspective, the information environ-

115. See GEORGE LAKOFF & MARK JOHNSON, *METAPHORS WE LIVE BY* (1980); GEORGE LAKOFF & MARK JOHNSON, *PHILOSOPHY IN THE FLESH: THE EMBODIED MIND AND ITS CHALLENGE TO WESTERN THOUGHT* 16–59 (1999).

ment is defined by the sum total of these activities and is experienced spatially, in terms of the freedom of movement it permits.¹¹⁶ Processes of information access and use within this environment are not entirely purposive, but are structured importantly by chance encounters and fortuitous juxtapositions. Situated, embodied users appropriate the information that they encounter for inter-linked purposes of consumption, communication, self-development, and creative play, and the result of these behaviors is the larger landscape of cultural and communicative activity.¹¹⁷

Pervasively distributed copyright enforcement portends fundamental change in these processes. The linked regimes of authorization and constraint will constrict the “breathing room” that is a critical constituent of each of them. The interpolation of pervasively distributed copyright enforcement into formerly private spaces redraws the experienced boundary between private and public, producing at the intersection a third sort of space that is neither entirely private nor conventionally public. The practice of intellectual consumption under a regime of pervasively distributed copyright enforcement seems likely to combine the exposure of behavior in public spaces (but not the expressive privileges) with the isolation of private spaces (but not the security against intrusion).¹¹⁸ Although concerns about the inviolability of personal spaces are often couched in the language of privacy rights, that language seems insufficient to comprehend these changes. The interpolation of copyright enforcement functions into private spaces, and private intellectual activities conducted from within those spaces, works a kind of displacement that is no less real because it is nonphysical.

At both the individual level and the network level, pervasively distributed copyright enforcement seeks to produce standardized, predictable flows of information. Michael Madison has argued that, just as early twentieth-century urban planning moved to eliminate visual chaos and replace it with order, so the technical and contractual mediation of information flows threatens to eliminate the diversity of textures and “feels” that flourishes under less restrictive architectures.¹¹⁹ This insight reaches beyond “information” abstracted from time and

116. See generally Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. (forthcoming 2007) (arguing that the networked information environment is experienced in terms of embodied spatiality).

117. See Julie E. Cohen, *The Place of the User in Copyright Law*, 74 FORDHAM L. REV. 347, 370–73 (2005).

118. Donna Haraway provides an evocative account of the relation between information flows and the spaces of the body, and of the ways that this relation might be shaped by an “informatics of domination.” DONNA J. HARAWAY, *SIMIANS, CYBORGS, AND WOMEN* 149–81 (1991). She observes: “One should expect control strategies to concentrate on boundary conditions and interfaces, on rates of flow across boundaries Human beings, like any other component or subsystem, must be localized in a system architecture whose basic modes of operation are probabilistic, statistical. No objects, bodies, or spaces are sacred in themselves” *Id.* at 163.

119. Michael J. Madison, *Complexity and Copyright in Contradiction*, 18 CARDOZO ARTS & ENT. L.J. 125 (2000); cf. Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 WASH. & LEE L. REV. 93 (2005) (noting this risk in the context of RFID-based information systems and

place, and indeed, on its own terms, it must reach more broadly. The shifting of intellectual activities into the controlled and authorized spaces of pervasively distributed copyright enforcement is in some respects comparable in feel to the replacement of mixed-use urban landscape with a large shopping mall or housing development. If these changes are to operate, as we are told they must, upon the entire information landscape, the scope of the resulting dislocation will be enormous.

If one keeps in mind that the central concern of pervasively distributed copyright enforcement is discipline as opposed to simple prohibition, none of this should come as a great surprise. Foucault reminded us that geographic segregation, rank-ordering, and internalization can be effective disciplinary substitutes for more extreme measures of social control. Nonetheless, the techniques of pervasively distributed copyright enforcement betoken a qualitative shift in the extent and nature of the structuring process that operates at the “normal” end of the spectrum. As already noted, moreover, state sovereigns are not indifferent to the possibility of inserting control and surveillance functions into communications networks. In the realm of online communication, disciplinary regimes designed for one purpose can easily be adapted to others. Embedded controls that identify and locate information users also lend themselves well to the reproduction of territorial sovereignty.¹²⁰ The adaptation and territorialization of control and surveillance functions can empower sovereigns to combat purely local plagues—terrorism, or pornography, or hate speech, or dissent. Through pervasively distributed copyright enforcement, state sovereigns may realize their own dreams of control, and far more easily than they could have done directly.

Here, however, we come to the speech libertarian objection: Surely it is going a bit far to say that the normalization of crisis mode strips individuals of whatever agency and private space they possess? There is, after all, a certain irony in structuralist defenses of individual freedom.¹²¹ If we are to take individual freedom seriously, must not we also take seriously the individual capacity to resist rules and practices that seem unwarranted and unjust? In particular, as poststructuralist critiques of intellectual property law reiterate, the mere fact that society adopts rules to govern the permissible use of intellectual property by no means ensures that individuals will obey them. Individuals are not simply passive recipients of cultural goods, but construct their own meanings by acts of resistance and appropriation.¹²² If new obstacles to these

arguing that these systems should be designed and implemented in a way that fosters diversity of sources, viewpoints, and uses).

120. See Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 JURIMETRICS J. 26 (2002).

121. For a particularly insightful version of this critique, see DAVID LUBAN, *LEGAL MODERNISM* (1997).

122. See ROSEMARY J. COOMBE, *THE CULTURAL LIFE OF INTELLECTUAL PROPERTIES: AUTHORSHIP, APPROPRIATION, AND THE LAW* (1998); Negativland, *Two Relationships to a Cultural Public Domain*, 66 LAW & CONTEMP. PROBS. 239 (2003); David Lange & Jennifer Lange Anderson, *Copyright, Fair Use and*

practices appear, individuals will find ways around them. Here the poststructuralist critique achieves an unlikely fusion with a distinctly cyberlibertarian vision of the agency of information users: If pervasively distributed copyright enforcement is this bad, people will refuse to accept it, and if it is foisted upon them, they will sabotage it. In addition, the strategies described in Part I have catalyzed the emergence of what one might characterize as “pervasively distributed copyright resistance”¹²³: a diverse, decentralized set of efforts to counter, undermine, and reverse the initiatives on which pervasively distributed copyright enforcement relies.

In the literal sense, this critique is quite right. Many of the measures described above are aspirational; there are no guarantees that they will find acceptance among information users and technology providers and no guarantees that they will work as claimed. Most likely, even universal implementation of the full range of enforcement measures sought by the entertainment industries will not ensure their universal success, and will fail to produce perfect regularity of discipline within the information environment. Technically-skilled risk-takers will be able to hack the code, defeat the watchers, and nurture thriving darknets. Some will choose open source systems and will develop ways to spoof the hard-wired detectors. And some will become passionate, dedicated advocates for resistance, reframing, and reversal. Perfect panopticism, in other words, is unattainable. The digital world will remain an arena in which conflicting spatial practices and visions struggle for primacy.

Preventing all unauthorized uses of information, however, is not the point of pervasively distributed copyright enforcement, just as preventing every single death was not the point of medieval plague control regimes and preventing every single crime is not the point of prisons. The opposite is more nearly true; as Foucault explained, to perform its function as a mechanism of social discipline the modern penal system requires crime, or at least criminals, in steady supply.¹²⁴ Normal discipline requires deviance constantly produced and carefully defined. Normalized crisis management adopts as an additional leitmotif the specter of barely averted, always imminent collapse. The darknet serves both needs.

The interplay between authorized uses and the darknet will recast the options available to both ordinary and technically-skilled information users. As Rosemary Coombe has explained, the rules that govern the use of intellectual goods can expand or constrict the available scope for the construction of difference through creative appropriation.¹²⁵ In conditions of postmodernity, which have been characterized in part by the accumulation of informational capital and its exchange via global communications networks, these rules have trended inexora-

Transformative Critical Appropriation (2001) (unpublished manuscript, on file with author), available at <http://www.law.duke.edu/pd/papers/lingeand.pdf>.

123. Thanks to Michael Birnhack for supplying this term.

124. See FOUCAULT, DISCIPLINE AND PUNISH, *supra* note 70, at 82–103.

125. COOMBE, *supra* note 122.

bly toward increasing constriction even as the popular claim of right to engage in acts of creative (or destructive) appropriation has become more acute.¹²⁶ This is doubly true of the technical and contractual mechanisms that extend automated enforcement into the spaces of intellectual consumption, and therefore affect not only the legality but also the literal feasibility of resistance. Pervasively distributed copyright enforcement operates upon difference and resistance to produce homogenous, abstract, carefully controlled space, within which even difference and resistance follow more narrowly prescribed paths.¹²⁷

More generally, the rules that shape the spaces of intellectual consumption can expand or constrict the available scope for law- and norm-creating activities by private individuals and their communities. This dynamic is starkest in the case of automated enforcement effectuated by surface-level restrictions and trusted systems. Automated enforcement via authorization and constraint elides the difference between public/rule-governed behavior and private behavior that is far more loosely circumscribed by applicable rules and social norms.¹²⁸ Some offenses, most notably crimes against persons, are so severe that they may be thought to justify such elision.¹²⁹ In other cases, though, we might conclude that looseness of fit between public rules and private behavior is itself a social good. Where the precise contours of legal rules are unclear, or the proper application of legal rules to particular facts is contested—which is to say, in most cases—imperfect control of private conduct shields a range of experimentation that involves individuals and communities in the creation of law and furthers the value-balancing goals of a sound and inclusive public policy.¹³⁰

For all of these reasons, neither the postmodern counterhegemon nor the law-creating citizen fares especially well under the sort of regime that pervasively distributed copyright enforcement seeks to instantiate. Crisis management mediated through and by the information environment narrowly circumscribes the possibility for opposition, deliberative dialogue, and everything in between. These costs of pervasively distributed copyright enforcement should not lightly be dismissed as insignificant, or as wholly subject to nullification through interstitial strategies of resistance. From the standpoint of informa-

126. See COOMBE, *supra* note 122, at 47–52. As Yochai Benkler demonstrates, these are not necessary conditions of an information-based economy. See YOCHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* (2006). But they are the conditions that have predominated so far.

127. Cf. HENRI LEFEBVRE, *THE PRODUCTION OF SPACE* 319–20 (Donald Nicholson-Smith trans., Blackwell 1991) (1974) (“[I]n a brightly illuminated night the day’s prohibitions give way to profitable pseudo-transgressions.”).

128. An earlier version of the argument in this paragraph appears in Cohen, *supra* note 102, at 587–88.

129. It is worth noting, however, that we are far from certain about this. In particular, ANTHONY BURGESS, *A CLOCKWORK ORANGE* (1962), is a powerful manifesto against the use of behavioral engineering to constrain volition in precisely the circumstances that might be considered most compelling.

130. See Robert M. Cover, *The Supreme Court, 1982 Term—Foreword: Nomos and Narrative*, 97 HARV. L. REV. 4 (1983).

tion users, all of this seems rather a large price to pay for better copyright enforcement, more orderly information markets, and the stabilization of norms about information use.

Here, though, it is necessary to consider the views of a final group of critics: those who believe that the rhetoric of crisis is apt and that a shift to crisis management is the only defensible response. This belief need not rest solely on economic self-interest; many believe that a healthy system of copyright protection and the system of market production that it enables are essential prerequisites for expressive liberty and so for intellectual self-determination.¹³¹ If there is indeed a crisis, and if pervasively distributed copyright enforcement is the best way to manage it, the price may seem inevitable. Neither proposition is certain. From a practical standpoint, however, the latter proposition seems both more important and more amenable to reasoned evaluation. Part V discusses the considerations that should inform this inquiry.

V. TAKING IMPERFECTION SERIOUSLY

I have argued that pervasively distributed copyright enforcement supplies a novel template for social discipline in the information age, and one that we ought to think twice about. Crisis management seems most essential, and interstitial strategies of resistance most significant, if there is no other way to achieve an acceptable balance between protection of intellectual content and preservation of personal liberties. The proper balance between enforcement and restraint is an age-old question in market-democratic societies, and solutions have always entailed compromise. It would be odd if the advent of digital networked technologies altered this dynamic so completely that middle-ground possibilities ceased to exist. If so, then our choices are far richer than we have been led to believe, and do not reduce to a stark election between pervasively distributed copyright enforcement and information anarchy.

At this point, however, I may seem to be trapped in a dilemma of my own making. I have argued that the form of discipline that pervasively distributed copyright enforcement represents is both qualitatively different from earlier modes of discipline and normatively undesirable. In the networked information age, it is inevitable that we will have a form of discipline that incorporates some form of regulation-by-protocol and therefore presupposes some degree of coordination. If the political critique that I have offered applies equally to all forms of regulation-by-protocol, we are in trouble. In particular, it is difficult to see how one might reconcile the argument made in Part II with the argument made in the previous paragraph, which contemplates the existence of a productive middle ground.

My answer to this question is a Foucauldian one: Some form of discipline we

131. The now-classic version of this argument is Neil Weinstock Netanel, *Copyright and a Democratic Civil Society*, 106 *YALE L.J.* 283 (1996). See also TYLER COWEN, *IN PRAISE OF COMMERCIAL CULTURE* (1998) (arguing that market economies foster artistic vitality and diversity).

must have. The political implications of a shift to regulation-by-protocol can be minimized only by commitment to what in Foucauldian terms might be characterized as an ethic of problematization: a commitment to uncovering and interrogating the systems of categorization and valuation implicit in patterns of social ordering, and to demonstrating that they are neither natural nor inevitable.¹³² This process in turn opens the way for new, as-yet-unpredicted patterns of ordering to emerge. In the age of regulation-by-protocol, an ethic of problematization must focus not only on the social construction of knowledge, but on the social construction of technical design.

Architectural regulation has a dual character. It is both a qualitatively different mode of regulating conduct and a mode of regulation that encompasses a continuum of regulatory effects. As an example, consider the conventional practice of engineering cars to prevent them from being driven above a certain speed. Formally, speed exists on a continuum. As a practical matter, however, it matters enormously—*qualitatively*—whether the hardwired maximum is set to equal the legal speed limit or, say, 110 miles per hour. The first solution is a form of crisis management; it leaves no room to go faster even when doing so would ease traffic flow or save lives. The second preserves both literal freedom of movement and a corresponding moral and political agency. In the context of speed controllers, we understand the difference well. But the problem is easy precisely because the regulation is so crude. Regulation-by-protocol is capable of immensely greater precision than other sorts of architectural regulation,¹³³ but it does not follow that this capability should therefore be developed to its fullest extent. We are not as good at understanding where and how algorithmic precision shades into coercion. Instead, as the current vogue for regulation-by-protocol demonstrates, we are peculiarly vulnerable to the seductive rationality of approaches that combine precise architectural targeting with other, subtler forms of behavioral engineering. Consider now the current debate about the practice of engineering rental cars to report driving over a designated maximum speed, and then automatically levying large penalties against those renters.¹³⁴ This is a regime of crisis management that differs from regulation-by-speed controller only in its sophistication. Formally, it leaves agency in place; practically, however, it seeks to harness and normalize patterns of authorization and constraint to produce drivers who exercise agency only within substantially narrowed confines.

132. See, e.g., Foucault, *supra* note 91, at 222–26 (outlining a method for the analysis of power relations within society).

133. Cf. James Grimmelmann, *Regulation by Software*, 114 *YALE L.J.* 1719, 1730–32 (2005) (arguing that software is characterized by greater “plasticity” than physical architecture and therefore is a separate regulatory modality in its own right).

134. See Ian Ayres & Barry Nalebuff, *Connecticut’s Speeder-Friendly Crackdown*, *N.Y. TIMES*, Aug. 31, 2001, at A19; Anita Ramasastry, *Tracking Every Move You Make: Can Car Rental Companies Use Technology to Monitor Our Driving?*, *FINDLAW’S WRIT* (Aug. 23, 2005), <http://writ.news.findlaw.com/ramasastry/20050823.html>. I thank David McGowan for this example, especially because it proves more than he thinks it does.

In the largest sense, the question that needs to be answered is whether the technology-based strategies of pervasively distributed copyright enforcement can be said to be “inherently” authoritarian, in the sense that their deployment and administration presuppose and reproduce authoritarian social structures, or whether these technologies might have implementations that are compatible with the preservation of a broader range of individual freedoms and a broader diversity of information spaces.¹³⁵ Both Lessig and Galloway seem to think the latter. For Lessig, anti-authoritarianism subsists in those protocols that are least amenable to centralized control and most transparent to end users.¹³⁶ For Galloway, it subsists in patterns of flow that are “rhizomic”: that are immanent in structure rather than predetermined by authority.¹³⁷ But both appear to believe that absent coordinated legal intervention on behalf of powerful, rent-seeking industries, market or extramarket forces would drive toward this result. I have argued that we should not necessarily expect this outcome, and that the forces pushing toward the instantiation of crisis management are exceptionally powerful precisely because they are decentralized.

The dynamic described in Part III suggests that if we are to avoid authoritarian forms of regulation-by-protocol, the parameters that enable anti-authoritarian outcomes must be designed. This conclusion may seem to frame a second, equally irreconcilable dilemma. It may seem that to talk about the design of discipline is necessarily to engage in an authoritarian enterprise.¹³⁸ This objection is enormously important. To reconcile design with freedom, it will be necessary to think about and practice design in a different way than we are used to doing. In that spirit, I would like to close by putting two questions on the table, one theoretical and one practical.

On the theoretical level, designing for imperfect control of individual behavior requires a rigorous inquiry into the location of the boundary between regulation and coercion, and into the normative justifications for choosing imperfection rather than simply settling for it. Much important work has been

135. This framing of the determinism question is Langdon Winner's. See LANGDON WINNER, *THE WHALE AND THE REACTOR: A SEARCH FOR LIMITS IN AN AGE OF HIGH TECHNOLOGY* (1986); see also WINNER, *supra* note 74, at 325–35 (calling for an “epistemological Luddism” that would consider “at least the following: (1) the kinds of human dependency and regularized behavior centering upon specific varieties of apparatus, (2) the patterns of social activity that rationalized techniques imprint upon human relationships, and (3) the shapes given everyday life by the large-scale organized networks of technology”). For preliminary explorations of this question in the context of DRM technologies, see Timothy K. Armstrong, *DRM and the Process of Fair Use*, 20 HARV. J.L. & TECH. (forthcoming Fall 2006); Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41 (2001); Deirdre Mulligan & Aaron Burstein, *Implementing Copyright Limitations in Rights Expression Languages*, in *DIGITAL RIGHTS MANAGEMENT: ACM CCS-9 WORKSHOP, DRM 2002*, at 137 (Joan Feigenbaum ed., 2003).

136. LESSIG, *supra* note 74.

137. GALLOWAY, *supra* note 90.

138. Cf. Mark Tushnet, “*Everything Old Is New Again*”: *Reflections on the “New Chicago School,”* 1998 WIS. L. REV. 579 (arguing that proposals for norm engineering are inconsistent with classical liberal policy of distinguishing between conduct, which may be punished, and belief, which may not be punished).

done on these questions.¹³⁹ Yet much more remains to be done. In the age of regulation-by-protocol, theoretical justifications for choosing imperfection must be carefully linked to the practices, spaces, and contexts within and through which individuals experience the information environment, and the ways in which authorization and constraint alter those experiences. An example of a literature that attempts this sort of task is the postmodernist literature on architecture and the event, which attempts to articulate in a systematic, concrete way both the experienced connections between architecture and constraint and the case for disrupting settled expectations about how we live just enough that new patterns of living might emerge.¹⁴⁰ This does not mean that event theorists advocate or seek to produce chaos; rather, they seek to encourage thinking differently about the relationship between physical structure and social structure, and about the ways in which physical structure both creates possibility and forecloses impossibility. Cautioning that prediction too is a form of control, they focus on the ways in which discontinuity and disjunction in the built environment might leave room for the impossible (judged against current referents) to emerge. These principles are well-suited to inform the design of intellectual space; what is needed here is a formal, detailed elaboration of the relationship(s) between the structure of experienced space and the processes of artistic and intellectual exploration.¹⁴¹

On the practical level, designing for imperfection requires specifying concrete parameters for enabling conduct that cannot be predicted or even imagined in advance. This requires a reversal of the current emphasis on enhancing the precision of digital delivery systems. A general model for the sort of effort that I have in mind may be found in the movement toward value-centered design, which stresses the iterative articulation of and engagement with normative values throughout the design process.¹⁴² Adapting this model to the task of

139. See, e.g., BENKLER, *supra* note 126; JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY (1996); COOMBE, *supra* note 122; LESSIG, *supra* note 74; LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY (2004); JESSICA LITMAN, DIGITAL COPYRIGHT (2001); Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1 (2004); Boyle, *supra* note 75; Boyle, *supra* note 78; Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996); Niva Elkin-Koren, *Cyberlaw and Social Change: A Democratic Approach to Copyright Law in Cyberspace*, 14 CARDOZO ARTS & ENT. L.J. 215 (1996); Reidenberg, *supra* note 74; Samuelson, *supra* note 16.

140. See, e.g., JOHN RAJCHMAN, *What's New in Architecture?*, in PHILOSOPHICAL EVENTS: ESSAYS OF THE '80s 152 (1991); BERNARD TSCHUMI, ARCHITECTURE AND DISJUNCTION (1994).

141. For efforts in this direction, see Julie E. Cohen, *Copyright, Commodification, and Culture: Locating the Public Domain*, in THE FUTURE OF THE PUBLIC DOMAIN 121, 146–60 (P.B. Hugenholtz & L. Guibault, eds. 2006); Julie E. Cohen, *Creativity and Culture in Copyright Theory*, 40 U.C. DAVIS L. REV. (forthcoming 2007); Jessica Litman, *Sharing and Stealing*, 27 HASTINGS COMM. & ENT. L.J. 1 (2004); Jessica Litman, *Lawful Personal Use* (unpublished manuscript, on file with author), available at <http://chicagoip.com/lawfulpersonaluse.pdf>.

142. See generally BATYA FRIEDMAN, PETER H. KAHN, JR. & ALAN BORNING, VALUE SENSITIVE DESIGN: THEORY AND METHODS (2002), <ftp://ftp.cs.washington.edu/tr/2002/12/UW-CSE-02-12-01.pdf>; BATYA

designing for imperfection, however, requires pushing beyond more specific normative visions, which tend to presuppose a degree of predictability, toward strategies for encoding gaps within which the impossible might emerge.

Here is an example of the sort of thing I don't mean to suggest¹⁴³: Many designs for surface-level technical protections now explicitly incorporate a degree of "wiggle room" for the user. For example, a song downloaded from Apple's iTunes store can be saved to five different computers,¹⁴⁴ and this feature has been hailed as a turn toward more consumer-friendly technological protection. That may be so, but it doesn't herald a turn toward the other sorts of constitutive freedoms that I have described. We still know where all of the copies are, and we have a pretty good idea how they are being used. To that extent, the iTunes platform is a digital Disneyland; it is play carefully engineered and tightly controlled. The iTunes platform also allows users to burn unlimited copies of songs to CDs and to rip unprotected mp3 files from the CDs.¹⁴⁵ This feature comes closer to enabling constitutive freedoms, but the terms of Apple's clickwrap license appear to prohibit many of the actions that users might wish to take.¹⁴⁶ And if CDs and CD burners go the way of analog cassette tapes, or are redesigned to behave differently, the theoretical freedom to "burn, rip, and mix" would be much less significant as a practical matter. What this example tends to suggest, then, is that even when we think we are choosing imperfection, we may not really mean it. Wiggle room and freedom of movement are not the same. Consumptive freedom is important, but it is not the only sort of freedom with which copyright policy and more broadly political theory should be concerned. Choosing imperfection requires the deliberate design and implementation of systems that incorporate far more tolerance for freedom of movement, and that therefore enable digital files to be accessed, copied, and used in as-yet-unpredicted ways.¹⁴⁷

Here are some examples of the sort of thing that I do mean to suggest: If wholly uncontrolled global distribution is the problem, set permissions levels so high that the limits would constrain only users who attempt to share hundreds or even thousands of copies; the resulting freedom to copy would enable some "merely" consumptive use, but also might afford fortuitous inspiration to the

FRIEDMAN, VALUE-SENSITIVE DESIGN: A RESEARCH AGENDA FOR INFORMATION TECHNOLOGY (1999), http://www.ischool.washington.edu/vsd/files/friedman99VSD_Research_Agenda.pdf; HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY (Batya Friedman ed., 1997) (collecting essays and case studies that explore the intersection between human values and technical design).

143. Although some of my earlier work may fairly be read to suggest it. See Burk & Cohen, *supra* note 135.

144. See BERKMAN CTR. FOR INTERNET & SOC'Y AT HARVARD LAW SCHOOL, DIGITAL MEDIA PROJECT, *iTUNES: HOW COPYRIGHT, CONTRACT, AND TECHNOLOGY SHAPE THE BUSINESS OF DIGITAL MEDIA—A CASE STUDY* 11–16 (Berkman Publ'ns Series No. 2004-07, 2004).

145. See *id.*

146. See *id.* at 15–16.

147. Cf. Armstrong, *supra* note 135, at 5–6 (calling for "systems that unlock the *process* of fair use"); *id.* at 46–53 (proposing an architecture that would allow user override of technical restrictions subject to an "identity escrow" requirement).

next Picasso or provide the tools for self-determination to the next Gandhi. If true “piracy” is the problem, link liability for the manufacture, distribution, or use of circumvention tools to an infringing purpose; the resulting freedom to tinker would enable both as-yet-unpredicted uses and the development of as-yet-unpredicted platforms and tools.¹⁴⁸ If exponentially enhanced anonymity of true “pirates” is the problem, deploy watermarking technologies to create audit trails that lead only partway to any individual user; the resulting freedom to behave badly would preserve moral and political agency while leaving content providers no better or worse off than they are with respect to efforts to discover and punish unauthorized analog reproduction. If malware is the problem, adopt open “trusted systems” standards that would enable multiple, competing providers to authenticate files and applications as “trusted”; the resulting freedom to compete would enable more precise differentiation between true threats and legitimate market alternatives.

Any of these approaches would entail not simply tolerating, but rather embracing, an enforcement equilibrium that includes a much higher proportion of unauthorized conduct, and for some that may make these approaches normatively undesirable for other reasons. The key point here, however, is not that such an equilibrium would be ideal either from the perspective of those who seek perfect control or from the perspective of those who seek perfect freedom, but rather that it still would fall well short of constituting “crisis” from either perspective. For exactly that reason, it would do a much better job of accommodating the competing goods that I have described.

148. See Samuelson, *supra* note 16.