

NORMAL DISCIPLINE IN THE AGE OF CRISIS

JULIE E. COHEN*

Abstract

As a byproduct of the asserted imperative to control flows of unauthorized information, purveyors of intellectual goods are moving to build into delivery systems for digital information a range of capabilities that insert both surveillance and enforcement functions into private spaces and embed these functions within communications networks, protocols, and devices. This essay offers a framework for theorizing this process that is informed substantially by the work of Michel Foucault and Anthony Giddens. The extension of intellectual property enforcement into private spaces and throughout communications networks can be understood as a species of disciplinary regime similar to those that Foucault sought to understand, but it is not exactly like any of those studied by Foucault. Instead, it represents a new, hybrid type, which locates the justification for its pervasive reach in a permanent state of crisis. Although the success of this hybrid disciplinary 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 this discipline in the 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 model of crisis discipline has profound implications for both the production of behavior and the production of information spaces, and raises pressing questions about the future of the networked information society.

* Professor, Georgetown University Law Center. Thanks to Bob Berring, Dan Burk, Susan Freiwald, Oscar Gandy, Mark Lemley, Clarisa Long, Mike Madison, Tom Nachbar, Ruth Okediji, Pam Samuelson, Marc Spindelman, Phil Weiser, Tim Wu, 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 and Matthew Windsor for research assistance.

NORMAL DISCIPLINE IN THE AGE OF CRISIS

INTRODUCTION

The drive toward technologically-assisted private ordering of rights in digital information is the subject of an enormous and growing theoretical literature. In particular, two dynamics – the enclosure of “intellectual property” and the erosion of online privacy – have received considerable attention. Much less attention has been paid to the ways in which the two dynamics overlap and intersect with one another. That subject, I will argue, deserves far more careful consideration. The interplay between the definition and enforcement of intellectual property rights and the development of practices and expectations regarding online privacy frames important choices about the kind of information society we want to have.

One might be tempted to think that the intellectual property-privacy intersection can be understood, relatively straightforwardly, as a special case of the more general surveillance-and-profiling dynamic. Digital delivery mechanisms for intellectual goods can enable increased collection of data about individuals’ informational preferences, which in turn can be used to tailor later informational offerings to those individuals. To a greater degree than some other kinds of profiling, profiling based on intellectual preferences raises the potential for political manipulation and the chilling of expressive and associative activities.¹ In general, however, one might conclude that the more sensitive ramifications of intellectual profiling can be addressed by devising special data processing protections for this sort of information. This understanding of the linkages between intellectual property and privacy is important, but incomplete.

The points of intersection between intellectual property and privacy do not primarily concern marketing, but also and more fundamentally discipline. As a byproduct of the asserted imperative to control flows of unauthorized information, purveyors of intellectual goods are moving to build into delivery systems for digital information a range of capabilities that insert both surveillance and enforcement functions into private spaces and embed these functions within communications networks, protocols, and devices. This process, which amounts to the privatization, automation, and pervasive distribution of intellectual property enforcement, is not simply about creating and rationalizing information flows within markets. It seeks to produce not only willing consumers, but tractable ones, and it seeks these changes not merely at the behavioral level, but at the cognitive level as well.

The framework that I will suggest for theorizing the extension of intellectual property enforcement into private spaces and throughout communications networks is informed substantially by the work of Michel Foucault and Anthony Giddens. This extension can be understood as a species of disciplinary regime similar in some respects to those that Foucault sought to understand. The particular disciplinary regime that these technologies represent, however, is not exactly like any of those studied by Foucault. Instead, it represents a new, hybrid type, which locates the justification for its pervasive reach in a permanent state of crisis.

¹ See Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at “Copyright Management” in Cyberspace*, 28 CONN. L. REV. 981 (1996).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

Although the success of this hybrid disciplinary 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 this discipline in the 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 model of crisis discipline has profound implications for both the production of behavior and the production of information spaces. Although the shift to crisis mode produces some undeniable benefits for information proprietors, it also works a violence that manifests in the disruption, invasion, and casual rearrangement of the boundaries of personal spaces, including both spaces of the body – homes, offices, and so on – and spaces of the intellect. The partitioning of information-related activity into discrete yet homogeneous disciplinary spaces threatens to produce, in turn, a larger geography of information space that is increasingly standardized. Important questions about the costs of this shift, and about alternatives, are swept aside in the push to institute perfect and conceptually crystalline control over information access and use. For precisely these reasons, the analysis developed here also has important implications for other areas of information policy, including most notably the ongoing debates about “tradeoffs” between privacy and network, commercial and national security. The emergent model of crisis discipline will produce spillover effects in all of these areas. As it does so, it will shape both practically and conceptually the construction of the networked information society.

I. LEVELS OF CONTROL

In an effort to prevent online copyright infringement, the major copyright industries and their technology partners are developing and implementing, and inducing third parties to develop and implement, a range of strategies that systematically shift the power to control or monitor individual practices of intellectual consumption toward purveyors of intellectual goods. These strategies include both technologies that monitor and restrict information use and rules broadly distributing responsibility for policing communications networks. Copyright industry members have exerted political, legal, and economic pressure on third-party providers of technologies and services that enable access to digital content to build similar technological capabilities into their own systems and into network standards, and more generally to serve as a “first line of defense” against unauthorized use. These initiatives may be envisioned as a series of concentric levels, each representing a more pervasive and invasive degree of control. As distinct from conventional representations of concentricity, in which successive layers build outward, the levels of control also press inward, into the logical and hardware layers of personal computers, home electronics equipment, and communications networks, leaving progressively less room to use informational content in ways that are both unconstrained and unobserved.

It is important to stress at the outset that at each of these levels, the implementation of control and surveillance functions is evolving and contested. What is presented here is a particular agenda of control developed and steadily advanced by the content industries over the course of the past decade. This agenda is consistent with, and has become an integral part of, the

NORMAL DISCIPLINE IN THE AGE OF CRISIS

larger agenda of commodification pursued by these industries. Whether this agenda will become reality, and to what extent, are questions that are yet to be determined. Many technically sophisticated observers believe that an uncontrolled “darknet” will always evade the content industries’ reach.² I take no position on whether that is so; 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.

A word first about terminology: the term now in vogue for the technologically-mediated control of access to and use of digital information is “digital rights management,” or “DRM.” Within copyright circles, this term has come to denote both the technologies that effectuate control and the positive theory of copyright law as default rules that underlies the quest to enable automated definition and management of digital “rights.”³ In a similar spirit, I will use “DRM” narrowly to refer to the technologies and processes of technologically-mediated control, but also more broadly to refer to the full panoply of coordinated initiatives directed at instantiating network-wide control of digital content and its users. Whether the term is used in its narrower or broader sense will, I trust, be clear from the context.

The first three levels of control over practices of intellectual consumption involve automated restrictions capable of implementation by copyright interests and their technology partners through licensing relationships with distributors. In most cases, these restrictions are also communicated to end users via complex, lengthy “licenses” that accompany the digital content. The first level consists of direct restrictions on what individuals can do, in the privacy of their own homes, with copies of works for which they have paid. The markets for digital music and movies offer the most prominent recent examples of delivery mechanisms designed to effectuate direct restrictions on user behavior. Within the past few years, members of the recording industry have test marketed several new CD releases in formats designed to prevent copying or “ripping” – converting musical selections to freely copiable computer files.⁴ Several new ventures in online music distribution, including Apple’s much-hyped iTunes program, are

² 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).

³ Both the positive theory and its normative implications are hotly debated. I will not recapitulate those debates here.

⁴ At least one early effort also prevented playback using a personal computer or accompanying peripheral device, and proved to be too drastic a change. See P.J. Huffstutter & Jon Healey, *Suit Filed Against Record Firms*, L.A. TIMES, June 14, 2002; Brenda Sandburg, *Milberg Weiss Files Suit Over CDs With No-Copy Technology*, THE RECORDER, June 17, 2002; Amy Harmon, *CD-Protection Complaint Is Settled*, N.Y. TIMES, Feb. 25, 2002, at C8. The current version of the technology allows 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 label has disclosed that planned upgrades will substantially reduce this 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>>.

NORMAL DISCIPLINE IN THE AGE OF CRISIS

offering downloads in proprietary formats tied to specific digital music devices.⁵ Movies distributed on DVD are encoded within a copy protection algorithm that prohibits play on any noncompliant DVD player; both DVD movies and DVD players also incorporate a system of “region coding,” designed to preserve geographic price discrimination, that prevents DVDs lawfully purchased on one continent from being played on equipment lawfully purchased on another.⁶ Other examples of direct restrictions include software copy protection that prevents a user from installing purchased software on more than one device in his or her home; region coding of popular video game programs; and copying restrictions encoded in software-based media players and e-book readers.

The second level of control over practices of intellectual consumption involves reporting back by the work (or, more precisely, by the software in which the copy of the work is embedded) on the activities of individual users. Such reporting may occur in conjunction with a pay-per-use arrangement for access to the work; for example, a licensed provider of Web-based music services might be required to monitor user consumption as a condition of its own license agreements with participating copyright owners. Alternatively, reporting may occur independently of payment terms. A surveillance mechanism might be designed to report attempts to make unauthorized copies, to detect and count non-copy-protected MP3 files, to determine what other computer programs a user is running in conjunction with a licensed program, or to monitor patterns of usage for marketing purposes. An example of this sort of surveillance system is the one designed by RealNetworks, a manufacturer of software for streaming music and video files. The software 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 player installed.⁷ Another example is the “SmartDownload” software included with a recent version of Netscape’s Communicator web

⁵ See Peter Lewis, *Drop a Quarter in the Internet*, FORTUNE, Mar. 22, 2004, at 56; Rob Pegoraro, *Apple Comes Closer to Perfect Pitch*, TECHNEWS.COM, May 4, 2003; see also Scott Banerjee and Brian Garrity, *Napster, Apple in Campus Deals*, BILLBOARD, July 31, 2004, at ___ (describing several major universities’ entry into partnership agreements with particular digital music services).

⁶ 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 Borland, *Studios Race to Choke DVD Copying*, CNET NEWS.COM, Feb. 4, 2002, <<http://news.com.com/2100-1023-828449.html>>. The copy-control and region-coding systems are administered by the DVD Copy Control Association, <<http://www.dvdcca.org/>>.

⁷ Greg Miller, *RealNetworks Breached Privacy, 3 Suits Contend*, L.A. TIMES, Nov. 11, 1999, at C1. Class actions filed in California, Illinois, and Pennsylvania by users who discovered their RealNetworks software “phoning home” charge that this conduct violated the federal Computer Fraud and Abuse Act and violated state law privacy rights. Amid the storm of protest that followed announcement of the lawsuits, RealNetworks rushed to disable its remote data collection capabilities, but maintained that it broke no laws. The courts ruled that the users’ grievances were covered by the arbitration clause included in RealNetworks’s “clickwrap” license. [MW: need final outcome info]

NORMAL DISCIPLINE IN THE AGE OF CRISIS

browser, which recorded every web site visited by users and transmitted that information back to Netscape.⁸

The third level of control of practices of intellectual consumption consists of attempts to impose vigilante justice on individuals believed to be intellectual property violators. For “authorized” content encoded with self-enforcing restrictions, enforcement protocols can be designed to encode penalties as well as disabilities. For example, a system could be designed that would disable access to digital content upon detecting an attempt at unauthorized use. The extent to which such “self-help” behavior should be permissible as a matter of contract law has been the subject of an ongoing dispute among drafters of a proposed uniform law to govern information transactions.⁹ Unauthorized, unprotected copies raise a different set of technical and legal considerations. Technically, it is possible to use peer-to-peer networks to deliver “logic bombs” designed to identify and destroy unauthorized files residing on users’ computers. As a legal matter, however, this conduct would implicate the federal Computer Fraud and Abuse Act, which prohibits unauthorized access to another’s computer system.¹⁰ The copyright industries have therefore supported legislation to create an exemption that would allow them to take the enforcement actions they desire.¹¹

Technologies that implement control, monitoring, and self-help functions effect direct regulation of user behavior. In addition, in 1998 the copyright industries secured passage of legislation, the Digital Millennium Copyright Act (DMCA), that provides two extra layers of legal protection for these technologies. The DMCA prohibits circumvention of technological measures that effectively control access to copyrighted works, and it also bans technologies that might enable copyrighted content to be stripped free of its protective coating.¹² The DMCA is law, not code; it does not physically or electronically prevent the spread of unprotected content or circumvention tools. Nonetheless, by placing the full force of the law behind private

⁸ See *Specht v. Netscape Communications Corp.*, 150 F. Supp. 2d 585 (S.D.N.Y. 2001), *aff’d*, 306 F.3d 17 (2d Cir. 2002) (holding that clickwrap agreement giving consent to the monitoring was unenforceable because of curable defects in contract formation)

⁹ Uniform Computer Information Transactions Act (UCITA) §§ 605, 815-816 (as amended 2002); UCITA §§ 605, 815-816 (as amended 2001); UCITA §§ 605, 815-816 (1999); Uniform Commercial Code (UCC) §§ 2B-310 and 2B-715, Reporter’s Note 3 (Aug. 1, 1998 Draft); UCC §2B-310, -716 (Apr. 1, 1998 Draft); UCC §2B-310, -716 (Feb. 1998 Draft).

¹⁰ See 18 U.S.C. § 1030.

¹¹ See H.R. 5211, 107th Cong., 2d Sess. (2002); Ted Bridis & Lee Davidson, *Download at Your Own Risk*, DESERET MORNING NEWS, June 18, 2003, at A01 (describing recent statements by Sen. Orrin Hatch supporting such an approach).

¹² Digital Millennium Copyright Act, Pub. L. No. 105-304, § 103, 112 Stat. 2860, 2863-76 (1998), *codified at* 17 U.S.C. § 1201.

NORMAL DISCIPLINE IN THE AGE OF CRISIS

technological ordering of intellectual consumption, it supports and ratifies industry-driven DRM initiatives. For example, the copy protection algorithm for DVDs has been broken, but it is unlawful to possess the decryption program, known as DeCSS, or to use it, make it directly available to others, or knowingly maintain links from which users could access sites offering it.¹³ DeCSS now resides on the darknet: it is undisputably still available, but at great potential cost. A 1996 treaty sponsored by the World Intellectual Property Organization obligates signatories to adopt laws that would produce similar effects.¹⁴

The fourth, fifth, and sixth levels of control of practices of intellectual consumption involve enforcement efforts directed at independent third parties who are perceived to be facilitating particularly high levels of infringement. Currently, large quantities of digital content are distributed in non-copy-protected form. Equipment and services provided by independent third parties – including digital video recorders, digital music players, CD and DVD burners, and Internet access accounts – give users considerable freedom to manipulate, share, and redistribute this content, and therefore work at cross purposes with copyright industry efforts at the first three levels. Accordingly, industry initiatives at the fourth, fifth, and sixth levels seek to block or control these other channels through which users might experience non-constrained, unmonitored content.

The fourth level takes the form of efforts to require independent third-party providers of equipment and/or content-related services to institute control or surveillance of user behavior. In several recent high-profile disputes, members of the copyright industries have sought to compel unwilling third-party providers to undertake policing and surveillance for them. The lengthy litigation involving the peer-to-peer file trading service known as Napster centered around recording industry efforts to require Napster to detect and block trading of copyrighted files. The court's remedial order stopped short of this result, but not by much, as it effectively required Napster to rewrite its operating software to detect and block any file identified to it as

¹³ 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 *Paramount Pictures Corp. v. 321 Studios*, 69 U.S.P.Q.2d 2023 (S.D.N.Y. 2004); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085 (N.D. Cal. 2004); *RealNetworks, Inc. v. Streambox, Inc.*, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000).

¹⁴ World Intellectual Property Organization Copyright Treaty, art. 11. Just how similar is a matter of some debate; 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 (2003). The point seems on the way to becoming moot, however, as many jurisdictions that have passed implementing legislation have followed the general approach of the U.S. model, either on their own initiative or as a result of bilateral trade agreements negotiated by the U.S. See U.S.-Singapore Free Trade Agreement, art. 16.4(7)(a); Australia-U.S. Free Trade Agreement, art. 17.4(7)(a); U.S.-Morocco Free Trade Agreement, art. 15.8(8)(a); see also Free Trade Area of the Americas Draft Agreement, art. 22 (Nov. 21, 2003).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

copyrighted.¹⁵ Unable to achieve a level of compliance with this order that would satisfy the recording industry plaintiffs, Napster eventually closed its doors. The Napster litigation was followed by a barrage of lawsuits against similar file-trading services.¹⁶ Meanwhile, in litigation over the ReplayTV video recording device, plaintiffs from the motion picture and television industries tried a different tactic. They requested, and convinced a magistrate judge to grant, a discovery order directing defendant SonicBlue to rewrite the ReplayTV software to generate information detailing subscribers' use of the device. That order was overturned, but SonicBlue later filed for bankruptcy in the face of mounting litigation expenses, and sold its ReplayTV technology and business.¹⁷ ReplayTV's new owners have removed two of the advanced capabilities that were the subject of the lawsuit: the ability to skip commercials automatically when recording and the ability to share recorded programming with other ReplayTV users.¹⁸ At present, litigation at this level is in some tension with a 1984 Supreme Court decision shielding third party device manufacturers from liability when their products are "capable of substantial non-infringing uses."¹⁹ The copyright industries are therefore seeking legislation that would effectively repeal that decision by establishing broad-based liability for "intentionally induc[ing]" infringement.²⁰

¹⁵ See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1027 (9th Cir. 2001) (allowing liability only to the extent that Napster had "reasonable knowledge of specific infringing files"); *A&M Records, Inc. v. Napster, Inc.*, 2001 Copr. L. Rev. ¶ 28,213 (N.D. Cal. Mar. 5, 2001) (entering preliminary injunction).

¹⁶ See *In re Aimster Copyright Litigation*, 252 F. Supp. 2d 632 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003), *cert. denied sub nom.* *Deep v. Recording Indus. Ass'n of Am.*, 124 S. Ct. 1069 (2004); *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029 (C.D. Cal. 2003), *appeal docketed*, Nos. 03-55894, 03-55901 (9th Cir. May 23, 2003).

¹⁷ Farhad Manjoo, *SonicBlue Freed From Monitoring*, WIRED.COM, June 3, 2002; Jon Healey, *Liberties Group Sues Studios Over Consumers' Use of Digital Devices*, L.A. TIMES, June 7, 2002; Jim Hu, *SonicBlue Seeks Bankruptcy Protection*, CNET NEWS.COM, March 21, 2003; Eric Hellweg, *SonicBlue's Bankruptcy: Score One for Big Media*, BUSINESS 2.0, March 26, 2003.

¹⁸ See Eric A. Taub, *ReplayTV's New Owners Drop Features That Riled Hollywood*, N.Y. TIMES, July 21, 2003, at C1. The ReplayTV web site maintains that it does not currently collect information about users' viewing habits, although it reserves the right to collect such information in the future.

¹⁹ *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984). Recognizing this, the courts have equivocated about the extent to which third party vendors must design their products to minimize copyright infringement. See *In re Aimster Copyright Litigation*, 334 F.3d 643, 653 (7th Cir. 2003), *cert. denied sub nom.* *Deep v. Recording Indus. Assn. of Am.*, 124 S. Ct. 1069 (2004); *A&M Records v. Napster, Inc.*, 239 F.3d 1004, 1020-21 (9th Cir. 2001). Most observers expect that the Court ultimately will be asked to revisit the *Sony* rule, if it is not legislatively repealed first.

²⁰ Inducing Infringement of Copyrights Act of 2004, S. 2560, 108th Cong., 2d Sess. (2004).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

The fifth level reinforces the fourth by targeting 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.²¹ 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.²² In another court, an online pornographer is suing an age verification service used by competitors that made copied, infringing materials available to their subscribers.²³ 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.²⁴

The sixth level of control involves efforts directed at third-party providers of network services. Some of these initiatives concentrate on removing unauthorized material from user Web sites and Internet search indices. In 1998, as part of the DMCA, the copyright industries won passage of legislation establishing a "notice and takedown" procedure under which online service providers, without judicial oversight, may remove material called to their attention by copyright owners in exchange for immunity from direct infringement liability.²⁵ Because the notice of infringement also creates the factual predicate for contributory infringement liability, service providers have a pressing incentive to comply.²⁶ The legislation also includes a subpoena provision designed to allow copyright owners to discover the identities of account-

²¹ 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 ___; 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, at ___.

²² UMG Recordings, Inc. v. Bertelsmann AG, 2004 U.S. Dist. LEXIS 13142 (N.D. Cal. July 14, 2004).

²³ 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, ___, 2004, at ___ (describing the same company's lawsuits against Visa and MasterCard for processing the payments).

²⁴ 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). The case was settled by confidential agreement.

²⁵ Digital Millennium Copyright Act, Pub. L. No. 105-304, § 502, 112 Stat. 2860, 2905-16 (1998), codified at 17 U.S.C. § 512.

²⁶ 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 (2003).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

holders who have posted infringing content, again without judicial oversight.²⁷ Although a federal appellate court recently ruled that recording industry plaintiffs may not rely on this provision as part of a more general effort to combat peer-to-peer file trading by linking U.S.-based IP addresses to specific users,²⁸ other avenues exist for discovering those users' identities. The industry has begun to file large numbers of so-called "John Doe" lawsuits against anonymous file traders, a procedural tactic that enables it to request judicially-supervised subpoenas directed to the online service providers whose services are being used.²⁹ In addition, it sent letters to the presidents of U.S. colleges and universities requesting that they begin monitoring student Internet accounts to detect peer-to-peer file trading activities, and followed up with an automated tool for processing takedown notices and disabling student access to peer-to-peer networks.³⁰ Still other initiatives are designed to insulate all users from unauthorized content by closing national borders to allegedly infringing traffic. Again, the recording industry has been the pioneer; in 2002, it 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. Exactly why the site disappeared remains a mystery.³¹

The final two levels of control of practices of intellectual consumption consist of attempts to shift both enforcement and surveillance functions progressively deeper into the logical and physical layers of the user's electronic environment.³² Along the way, these efforts recruit and implicate major sectors of the software, computer and communications industries.

²⁷ 17 U.S.C. § 512(h).

²⁸ *RIAA v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003). The recording industry is currently seeking a better result in a different forum. *See RIAA v. Charter Communications, Inc.*, No. 03-3802 (8th Cir. Nov. 20, 2003)

²⁹ *See Music Industry Sues 474 More People in Anti-Piracy Campaign*, ST. LOUIS POST-DISPATCH, June 23, 2004, at ___; JenMcCaffery, *Virginia Tech Computer User Is Sued By Recording Industry*, Roanoke Times & World News, Apr. 29, 2004, at A1 (describing 477 newly filed lawsuits); Nick Timiraos & Nicole Tingir, *RIAA Sues 3 Georgetown Students*, The Hoya, Mar. 26, 2004, at ___ (describing 532 newly filed lawsuits); Katie Dean, *RIAA Strikes Again at Traders*, Wired News, Jan. 21, 2004 (describing 532 newly filed lawsuits). For a collection of the pleadings and orders in many of these cases, see <<http://eff.org/IP/P2P/riaa-v-thepeople.php>>.

³⁰ *See American Council on Education, Higher Education Associations and the Creative Content Community Letters on P2P Piracy*, ACENET, Oct. 8, 2002, <<http://www.acenet.edu/washington/letters/2002/10october/copyright.cfm>>; Stefanie Olsen, *Hollywood's New Lesson for Campus File Swappers*, CNET NEWS.COM, Apr. 19, 2004.

³¹ Alex Pham, *Tactics Toughen on Music Piracy*, L.A. TIMES, Aug. 21, 2002; Kate Bulkeley, *New Media: Fair Play or Foul?*, THE GUARDIAN, Aug. 26, 2002.

³² The "layers" model originates with Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMM. L.J. 561 (2000).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

The seventh level seeks to implement DRM controls at the operating system layer. Microsoft's Next Generation Secure Computing Base project 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.³³ Other efforts to develop and implement controls at the logical layer are more collaborative, such as the Trusted Computing Platform Alliance (TCPA), a joint venture of Microsoft, Intel, IBM, Hewlett Packard, and Compaq; the Copy Protection Technical Working Group; and a project by the Organization for the Advancement of Structured Information Standards (OASIS) to develop open, non-proprietary standards for expressing and coding access control restrictions.³⁴

The eighth and final level of control of practices of intellectual consumption seeks to move the enforcement and surveillance functions into the physical layer, hard-wiring them into every kind of computing and home electronics equipment that an individual might employ to access copyrighted content. Should these initiatives succeed, the content- and device-specific restrictions observed at level one, such as the copy protection embedded within DVD players and disk drives, could give way to more universal hardware-driven regulation. Intel's LaGrande project is exploring the inclusion of control-enabling standards in the microprocessors used in personal computer systems.³⁵ Both the Microsoft and TCPA projects also have hardware-based components. The Federal Communications Commission is coordinating industry-based efforts to develop similar standards for digital broadcast and cable television; once agreed, these standards will be encoded in all digital television equipment.³⁶ The newest version of the

³³ See Neil McIntosh, *Online: Old Bill's Police Tactics*, THE GUARDIAN, July 4, 2002; Robert Lemos, *What's in a Name? Not Palladium*, CNET NEWS.COM, Jan. 24, 2003; Mary Jo Foley, *Microsoft: 'Palladium' Is Still Alive and Kicking*, EXTREME TECH.COM, May 6, 2004; *Palladium Operating System*, WIKIPEDIA, July 16, 2004.

³⁴ See Trusted Computing Platform Alliance, <<http://www.trustedcomputing.org/>>; Copy Protection Technical Working Group, <<http://www.cptwg.org/>>; OASIS, *Rights Language TC*, <http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=rights>.

³⁵ Chris Gaither, *Intel Chip to Include Antipiracy Features, Some Still Fear Privacy of Users Will Be Violated*, BOSTON GLOBE, Sept. 10, 2002, at C3; Nick Stam, *Inside Intel's Secretive 'LaGrande' Project*, EXTREME TECH.COM, Sept. 19, 2003; see also John Clyman, *Making Computing Trustworthy*, PC Mag., Nov. 11, 2003, at 97 (discussing both LaGrande and Microsoft's NGSCB).

³⁶ See Federal Communications Commission ("FCC"), *Digital Broadcast Content Protection: Notice of Proposed Rulemaking*, 68 FED. REG. 67,624 (Dec. 3, 2003); FCC, *Digital Broadcast Content Protection*, 68 FED. REG. 67,599 (Dec. 3, 2003); FCC, *Report and Order and Further Notice of Proposed Rulemaking*, No. 03-273 (Nov. 4, 2003); FCC, *Commercial Availability of Navigation Devices and Compatibility Between Cable Systems and Consumer Electronics Equipment*, 68 Fed. Reg. 66,728 (Nov. 28, 2003); FCC, *Second Report and Order and Second Further Notice of Proposed Rulemaking*, No. 03-225 (Oct. 9, 2003).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

Internet Protocol, IPv6, includes a so-called “stateful” mode that can facilitate persistent identification of Internet users.³⁷

For some intellectual property scholars, these initiatives are simply logical responses to the economics of large-scale infringement in a networked information environment.³⁸ That may be so (although I have my doubts), but the changes they portend for the networked information environment go far beyond allocative efficiency.

II. THE AGE OF ACCESS?

Theorizing the drive toward more perfect and more deeply-embedded control and surveillance of uses of digital content poses unique challenges for scholars accustomed to analyzing information markets within the framework of intellectual property policy. The emerging regime of control and surveillance is much more than simply a change in the structure of information markets. Information providers and information users will still transact, but information transactions will become fundamentally relational processes, mediated by complex and relatively opaque technical standards, that manifest as an incremental and increasingly severe loss of individual control over the parameters of personal space and personal intellectual activity. Nor is the progressive deployment of control and surveillance functions in markets for digital information exactly analogous to the process of standards development, although it requires the development of technical standards. Participation in both existing standards and standards development processes generally is determined by economic self-interest. In contrast, DRM initiatives are pointless unless compliance by equipment and service providers is mandatory. To understand the emerging regime of control and surveillance as a social and historical phenomenon, intellectual property scholars must look farther afield.

Jeremy Rifkin envisions the emerging information age as a web of mutually constituting access relationships that fulfill reciprocal needs.³⁹ Consumers, adrift in a sea of information,

³⁷ 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 underway 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.

³⁸ See, e.g., Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217; Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345 (forthcoming 2004); Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395 (2003); Randal C. Picker, *The Digital Video Recorder: Unbundling Advertising and Content*, 71 U. CHI. L. REV. 205 (2003).

³⁹ JEREMY RIFKIN, *THE AGE OF ACCESS: THE NEW CULTURE OF HYPERCAPITALISM WHERE ALL OF LIFE IS A PAID-FOR EXPERIENCE* (2000).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

benefit from establishing long-term relationships with information service providers. Information providers, in turn, need to form relationships with consumers as a way of competing successfully in the “attention economy.” This understanding of the information age as relational at its core is extremely important. Both within and outside markets, many exchanges of information look less like one-off transactions and more like a series of linked interactions, and the relationships established via DRM technologies and practices are intended to exploit and intensify this trend. Following on the work of Henry Maine, we might say that the information age represents a shift from contract, the market-forming mechanism of the nineteenth and twentieth centuries, to (contractually mediated) status.⁴⁰ But this observation in itself does not tell us much about the kinds of status that are created.

If the information age is an age of access, it is one in which notions of boundedness are applied unevenly, in ways that systematically deny private individuals entitlement to boundaries that information proprietors claim as a matter of course. Copyright entitlements have been extended in length, breadth, and depth, and augmented by rights against circumvention of access control measures. In disputes involving noncopyrightable information, courts have eagerly developed new theories to bar the “unauthorized” extraction of information from online repositories.⁴¹ At the same time, access to most personal information about individuals is presumptively uncontrolled, and courts have decreed that the new theories of unauthorized access that protect online commercial ventures do not bar the use of Web-based technologies to gather information about individual Internet users.⁴² Similarly, DRM enforcement and

⁴⁰ See HENRY SUMNER MAINE, *ANCIENT LAW* ____ (1861) (characterizing the rise of modern law as a shift from status to contract); see also CARL SHAPIRO & HAL R. VARIAN, *INFORMATION RULES* (1999) (outlining rules for commercial success in the emerging information economy); Margaret Jane Radin, *Online Standardization and the Integration of Text and Machine*, 70 *FORDHAM L. REV.* 1125 (2002) (discussing the tension between standardization and customization of contracts for access to information and information services).

⁴¹ See *EF Cultural Travel v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001); *Register.com v. Verio*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000); *eBay, Inc. v. Bidder’s Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000); Maureen A. O’Rourke, *Common Law and Statutory Restrictions on Access: Contract, Trespass, and the Computer Fraud and Abuse Act*, 2002 *U. ILL. J.L. & TECH. POL’Y* 295.

⁴² See *In re Pharmatrak, Inc. Privacy Litigation*, 220 F. Supp. 2d 4 (D. Mass. 2002); *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001) (cookies); *In re DoubleClick, Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (cookies); see also *Specht v. Netscape Communications Corp.*, 150 F. Supp. 2d 585 (S.D.N.Y. 2001), *aff’d*, 306 F.3d 17 (2d Cir. 2002) (holding that clickwrap agreement giving consent to monitoring of online activity by browser “plug-in” was unenforceable, but only because of curable defects in contract formation); John Borland, *A Secret War: Spike in “Spyware” Accelerates Arms Race*, *CNET NEWS.COM*, Feb. 24, 2003 (describing types and uses of web-based spyware technologies), <<http://news.com.com/2102-1001-964628.html>>.

NORMAL DISCIPLINE IN THE AGE OF CRISIS

surveillance initiatives operate on the premise that incursions into individuals' private spaces are both necessary and reasonable.⁴³

Alfred Yen has suggested that the emerging web of relationships between individuals and Internet access providers resembles a quasi-feudal regime of distributed governance.⁴⁴ 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."⁴⁵ Although in theory (and *in extremis*) an Internet access provider is subject to the full extent of state authority, 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 DRM enforcement and surveillance regimes.

The metaphor of the feudal fiefdom, however, seems imperfectly suited to describe the linked practices of control and surveillance of information use. 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. DRM technologies and related initiatives instead enable governability from afar. By insinuating automated control into formerly private spaces and activities, these technologies can obviate much of the need for localized enforcement. In theory, moreover, DRM regimes enable the coordination of regulation and surveillance by multiple right-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 distributed control and surveillance 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

⁴³ An exception to the DMCA's anti-circumvention provisions allows individuals to prevent the collection of information about their "online activities" when the DRM system does not provide "notice and opt-out" protection and the circumvention disables no other functions of the DRM system. 17 U.S.C. § 1201(i). It is unclear whether information about "online activities" includes information about individual use of the DRM-protected work. It is unlawful to create and offer to members of the public tools that they might use to exercise this right. *Id.* § 1201(a)(2), (b).

⁴⁴ Alfred C. Yen, *Western Frontier or Feudal Society?: Metaphors and Perceptions in Cyberspace*, 17 BERKELEY TECH. L.J. 1207 (2004); see also David D. Clark & Marjory S. Blumenthal, *Rethinking the Design of the Internet: The End to End Arguments vs. the Brave New World*, 1 ACM TRANS. INTERNET TECH. 70 (Aug. 2001).

⁴⁵ Yen, *supra* note ___, at 1240.

NORMAL DISCIPLINE IN THE AGE OF CRISIS

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.⁴⁶ Understanding these developments requires a theory that encompasses the modalities of regulation by pervasive, embedded social institutions.

III. CRISIS DISCIPLINE

Important tools for theorizing the progressive deployment of technologies for control and surveillance of intellectual consumption are found in the work of Michel Foucault.⁴⁷ Foucault sought to understand the workings of power within society, but not in the top-down sense with which the exercise of power is often understood. Instead, he focused on identifying and understanding 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.

Among Internet scholars, mention of Foucault in connection with the notion of institutions of societal discipline inevitably conjures up his work on so-called panoptic discipline. The Panopticon, devised by Jeremy Bentham as a model of the perfect prison, 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. Panoptic theories of the information age abound.⁴⁸ Panoptic references, however, sometimes strike critics as fantastic excursions into the realm of conspiracy theory. Some panoptic theorists take for

⁴⁶ 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., LANGDON WINNER, *AUTONOMOUS TECHNOLOGY: TECHNICS-OUT-OF-CONTROL AS A THEME IN POLITICAL THOUGHT* 323 (1983).

⁴⁷ MICHEL FOUCAULT, *POWER/KNOWLEDGE: SELECTED INTERVIEWS AND OTHER WRITINGS 1972-1977* (1980); MICHEL FOUCAULT, *DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON* (1975).

⁴⁸ See, e.g., OSCAR GANDY, *THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION* (1993); Stan Karas, *Privacy, Identity, Databases*, 52 AM. U.L. REV. 393 (2002); Stan Karas, *Enhancing the Privacy Discourse: Consumer Information Gathering as Surveillance*, 7 J. TECH. L. & POL'Y 3 (2002); Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297 (2004); JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* (2000); 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 (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). Within the legal literature on the shaping of the information age, the most sophisticated use of Foucauldian theory is James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

granted both motive and power to surveill and control human activity, and so do not explain the origins of the imperative to see. They explain how a particular configuration of social institutions might adapt to surveillance purposes, but not why it is likely (or even probable) that it might. Relatedly, panoptic theories often do not satisfactorily explain how the fundamentally centralized model of panoptic discipline translates to contexts in which neither surveillance nor control is centralized.

As these objections suggest, while the Panopticon was an interesting and memorably named conceptual experiment,⁴⁹ taken on its own terms it does not furnish a compelling model for many extensions of power in market-democratic societies. In particular, it does not provide a good model for understanding efforts by a loosely coordinated network of market actors to control the spread of unauthorized information online. To understand the impetus for the pervasive yet decentralized network of surveillance and control described above, we must begin with a more extensive survey of Foucault's study of the evolution and institutionalization of disciplinary norms.

Foucault studied both "normal discipline" and what I will call "crisis discipline." The former category encompasses 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. 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 – 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. 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 "polyvalent" 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."⁵⁰

⁴⁹ In fact, it was never built.

⁵⁰ FOUCAULT, DISCIPLINE AND PUNISH, *supra* note __, 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 __, at 185-88 (identifying the Panopticon as the "paradigm" for a model of disciplinary power).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

Crisis discipline, in contrast, refers to disciplinary regimes developed in response to extreme circumstances that were perceived to threaten the community's very survival. Unlike institutions 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.⁵¹ 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.

Technologies for distributed control and surveillance of intellectual consumption are intended, first and foremost, to instantiate crisis discipline in the Foucauldian sense. It may be objected that the highly physicalized, spatialized models of discipline described by Foucault have little application to the organization of information space. This objection, however, would be too hasty. Although information space does not permit direct physical contact, the current model of networked communication is regarded (by some) as proof that nonphysical contact too 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. 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,

⁵¹ FOUCAULT, DISCIPLINE AND PUNISH, *supra* note __, at 195-98.

NORMAL DISCIPLINE IN THE AGE OF CRISIS

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.⁵²

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.⁵³

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.⁵⁴

The phenomenon of online copyright infringement differs from a microbial epidemic in that 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. Extending the analogy, the deadly vector is not the protected work, but the unprotected work. Put more neutrally, the "propagated outbreak epidemic" to which Judge Kaplan referred is simply an example of a more general property of networks of all sorts⁵⁵; the content industries are not averse to harnessing the considerable

⁵² *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).

⁵³ See, e.g., *U.S. Senate Committee on Foreign Relations Holds Hearing on Evaluating International Intellectual Property Piracy*, FDCH POLITICAL TRANSCRIPTS, June 9, 2004 (testimony of Jack Valenti); Suzanne Choney, *Piracy Keeps Online Music From Singing a Happy Tune*, SAN DIEGO UNION-TRIB., May 3, 2004, at C-1; James Flanigan, *Asset-Heavy Companies Need to Slim Down*, L.A. TIMES, Jan. 19, 2003, at Business, p. 1; Olga Kharif, *Facing the Digital Music at Record Shops*, BUSINESSWEEK ONLINE, June 21, 2001, 2001 WL 25754353; Richard Shim, *News Corp. Exec Puts Piracy in the Spotlight*, CNET NEWS.COM, Nov. 19, 2002; <<http://news.com.com/2100-1040-966457.html>>; Tom Zucco, *Unchained Melodies*, ST. PETERSBURG TIMES, Sept. 30, 2002, 2002 WL 100422800; *Strategies to Sink the Music Pirates*, THE AUSTRALIAN, July 18, 2003, at 10; see also Lynden Barber, *Movie Piracy "Like Terrorism"*, AUSTRALIAN IT, Nov. 15, 2002.

⁵⁴ FOUCAULT, DISCIPLINE AND PUNISH, *supra* note ___, at 205.

⁵⁵ For a concise, highly readable explanation, see ALBERT-LASZLO BARABASI, LINKED: THE NEW SCIENCE OF NETWORKS 123-42 (2002).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

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 levels of control described above accomplish precisely this separation of protected from unprotected content, because they supply direct power over the use and transmittal of information goods. The technologies of constraint, surveillance, and automated self-help adapt the philosophy and instrumentalities of plague control to the digital age. Perfect surveillance of interactions with information goods obviates the need for physical confinement of persons, while direct functionality restrictions ensure that protected information carries the terms of its confinement with it. And direct functionality restrictions, surveillance, and automated self-help enable content proprietors to detect motion, and to kill that which moves only when that which moves is or would be unprotected.

IV. CRISIS, POWER, AND AUTHORITY

But how, exactly, does the emerging phenomenon of “crisis DRM” acquire the authority to subject practices of intellectual consumption to the instrumentalities of plague control? 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. As already noted, though, DRM technologies and related initiatives 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 discipline is an explanation of the logic that underlies the privatization and decentralization of disciplinary mechanisms in general, and crisis discipline in particular.

Answering these questions requires, first, some consideration of the origins of power, a problem in which Foucault himself seemed relatively uninterested.⁵⁶ 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.⁵⁷ Giddens substitutes a robust vision of human agency for the “docile bodies” of

⁵⁶ See, e.g., FOUCAULT, *POWER/KNOWLEDGE*, *supra* note ___, at 104-08.

⁵⁷ ANTHONY GIDDENS, *THE CONSTITUTION OF SOCIETY* (1984).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

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.⁵⁸ 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. Viewed through the lens of structuration theory, the drive toward extension of crisis DRM may be understood as flowing from the self-interested interactions of a number of relevant groups.

In the case of crisis DRM, the perceived need to control the threat of online copyright infringement supplies both information providers and governments with powerful (though slightly different) motives for surveillance and 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.⁵⁹ 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 far 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.

⁵⁸ Cf. PIERRE BOURDIEU, PRACTICAL REASON 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").

⁵⁹ See Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263 (2002).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

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 DRM technologies, and the notice-and-takedown provisions applicable to Internet service providers deliberately shift government out of the picture.⁶⁰ A legislative proposal to require all digital media devices to incorporate DRM controls, and to set federal guidelines for DRM standards, was ultimately rejected by a provisional coalition of technology and entertainment interests.⁶¹ The Federal Communications Commission's supervision of the broadcast flag and cable plug and play standards for digital television represents a departure from this pattern that is perhaps best explained by the history of more aggressive government oversight of broadcast and cable media. It is worth noting, moreover, that the House Judiciary Committee has warned the FCC to tread cautiously where copyright entitlements are concerned.⁶²

Here it is important to understand that the emerging network of private disciplinary measures serves both private and state interests far better than more extensive official involvement might. To the extent that crisis DRM remains primarily a matter of industry initiative, information providers enjoy virtually complete freedom to define the scope of their entitlements.⁶³ 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.⁶⁴ 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,

⁶⁰ See 17 U.S.C. §§ 512, 1201(a)-(b).

⁶¹ See Consumer Broadband and Digital Television Promotion Act, S. 2048, 107th Cong., 2d Sess. (2002).

⁶² See Drew Clark, *Intellectual Property: House Judiciary Asserts Jurisdiction in 'Broadcast Flag' Debate*, NAT'L J. TECH. DAILY, Mar. 6, 2003.

⁶³ For a similar analysis on this point, see Boyle, *supra* note __, at 197-98. 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).

⁶⁴ 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).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

quickly became mired in congressional hearings.⁶⁵ 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.⁶⁶ Among the USA PATRIOT Act's most maligned provisions is the one authorizing compelled, secret disclosure of library patrons' usage records.⁶⁷ Except among a small group of technological and legal cognoscenti, private-sector DRM initiatives have generated comparatively few ripples of alarm.

Deploying crisis discipline through the marketplace remains, nonetheless, a somewhat trickier business than deploying it by state fiat. A satisfactory explanation of the logic of crisis DRM must take into account the motives and practices of several additional groups of actors. Of these, the ultimate users of information goods are by no means the most important.⁶⁸

The "market for DRM" 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. 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, 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.

⁶⁵ See *Senate Rebuffs Domestic Spy Plan*, WIRED NEWS, Jan. 23, 2003; Jim Puzzanghera, *Senators Vow to Halt 'Data Mining' Project*, SILICONVALLEY.COM, Jan. 17, 2003. 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).

⁶⁶ See U.S. GENERAL ACCOUNTING OFFICE, *AVIATION SECURITY: COMPUTER-ASSISTED PASSENGER PRESCREENING SYSTEM FACES SIGNIFICANT IMPLEMENTATION CHALLENGES*, No. GAO-04-385 (Feb. 12, 2004); Alexandra Marks, *Big Business Joins Fight Against New Airport Screening*, CHRISTIAN SCI. MONITOR, Feb. 12, 2004, at 3; Jon Marino, *Fixes Promised For Planned Airport Screening System*, L.A. TIMES, Feb. 13, 2004, at A38; Mary Lou Pickel, *TSA Data Assertion Disputed by Delta*, ATLANTA JOURNAL-CONST., June 24, 2004, at 1D; 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.

⁶⁷ See 50 U.S.C. § 1861; Anne Klinefelter, *The Role of Librarians in Challenges to the USA PATRIOT Act*, 5 N.C.J.L. & TECH. 219 (2004); Eric Lichtblau, *U.S. House Deadlocks on Library Records Ban*, INT'L HERALD TRIB., July 11, 2004, at 21.

⁶⁸ Portions of the following discussion are adapted from Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 614-16 (2003).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

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 DRM mandates. They have been much less effective at resisting the incremental introduction of DRM functionality in newer technologies, such as DVD players, digital music and video game players, and software-based multimedia devices. In part this is 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 DRM initiatives reflects the fact that consumer expectations regarding new methods of distributing and rendering multimedia content are less fully formed. Acquiescing to content industry demands regarding copy-protection for DVD-based movies did not carry the same level of perceived marketplace risk as it did for CD-based music or free broadcast television.

The interplay of supply and demand in the market for DRM is further complicated by the dynamics of technical standardization. Because most copyright owners lack the technical expertise to build DRM technologies for themselves, computer technology companies and researchers play a pivotal role in the development and extension of crisis discipline.

Technical expertise vests its practitioners with an authority that is often confused with neutrality, but should not be. 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.⁶⁹ As in any other market, those purposes are determined at least in part by the customer. In the case of DRM standards, however, it is the large content industries, and to some extent Congress and the FCC, that developers must first aim to please. Unaffiliated and academic researchers are more likely to cast a critical eye on this process. Perhaps even more than their colleagues at for-profit companies, however, these individuals are highly motivated to solve the difficult theoretical problems that instantiation of DRM functionality requires.⁷⁰

As DRM standards penetrate more deeply into general purpose software and hardware, the mix of incentives, strategies, and habitual practice becomes even more complicated. In

⁶⁹ 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 __ (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 (1991).

⁷⁰ Cf. Bourdieu, *supra* note __, 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).").

NORMAL DISCIPLINE IN THE AGE OF CRISIS

particular, developers of computer operating systems and microprocessors must satisfy many groups of customers. Some developers, including most notably market leaders Microsoft and Intel, appear to believe that DRM capabilities mesh well with other design goals, such as enhanced network, server and file security. For Microsoft in particular, deployment of DRM functionality also seems bound up with a number of business-related objectives, including protection of its proprietary technical information and preservation of its market position. Other technical developers are less certain about the benefits of DRM functionality, but seek to avoid “technological mandates” from the government, and appear to perceive voluntary development efforts as the lesser of two evils.

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. Early versions of DRM technologies have provoked both kinds of user pushback. At higher levels of DRM penetration, however, both kinds of market resistance become more difficult. The more deeply embedded in software and hardware DRM standards become, the harder they are to avoid by purchasing noncompliant or alternative equipment. Particularly as more and more desired features and services are bundled with self-enforcing restrictions, the costs of opting out may rapidly come to outweigh the benefits. For all but a small group of technically skilled end users, more deeply embedded controls also are much harder to evade by circumvention.

At higher levels of DRM 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 formidable institutional obstacles to the development of open source media players that incorporate DRM functionality. Industry-sanctioned DRM 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.⁷¹ 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;

⁷¹ 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/ValentiIntervie.20f.html>>.

NORMAL DISCIPLINE IN THE AGE OF CRISIS

in any case, that exception also forbids widespread sharing of the information gained from reverse engineering.⁷²

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 crisis DRM long before implementations surface in the consumer marketplace, the closed nature of many DRM standard-setting processes, and the technical complexity of the subject matter.⁷³ 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 DRM standards.

Finally, the ideology of the marketplace itself reinforces the extension of crisis DRM, 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 control and surveillance, so privatized control and surveillance reinforce the 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 crisis DRM, 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 the ideology of crisis DRM 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 the development and deployment of crisis DRM 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. In important and mutually reinforcing ways, the recursive practices of market actors lend authority to the technologies of crisis control.

⁷² See 17 U.S.C. § 1201(f); *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).

⁷³ For a more extensive discussion of these considerations, see Cohen, *supra* note __ at 615-16; *cf.* GURAK, *supra* note __, at 66-83 (describing how the technical complexity of the issues surrounding deployment of the Clipper Chip created obstacles to the generation of a protest movement).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

As we shall see next, these technologies instill more than simply crisis discipline in the Foucauldian sense.

V. NORMALIZING EXIGENCY

Foucault's theory of crisis discipline also does not entirely explain the perceived need to hard-wire DRM controls. Emergencies pass, and with them the justification for the extreme measures they are 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. Thus, based on Foucault's work we might expect to see the ground being prepared for transition from a regime of crisis controls to a more relaxed regime once the immediate threat has passed. Yet plans for the progressive penetration of DRM protections into ever-deeper layers of personal computing and communications systems do not seem to contemplate a loosening of control.

This brings us to another important difference between online copyright infringement and microbial contagion: The sense of emergencies as episodic and temporary does not translate well to the context of online copyright infringement. Judge Kaplan, at least, does not seem to think that the digital plague of copyright infringement can be so easily eradicated:

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.⁷⁴

What happens to disciplinary modalities when crisis is not temporary, but a permanent state of affairs? As Foucault explains, a 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."⁷⁵ These disciplinary methods work, in other words, because citizens of a society internalize the criteria that they apply. Normal discipline

⁷⁴ *Reimerdes*, 111 F. Supp. 2d at 332.

⁷⁵ FOUCAULT, DISCIPLINE AND PUNISH, *supra* note __, at 205.

NORMAL DISCIPLINE IN THE AGE OF CRISIS

labels and smooths away quotidian challenges to the fabric of social life. We carry our conditioning, and our blinders, with us. What, though, is normal discipline in an age of crisis?⁷⁶

If the sense of continuing crisis articulated by Judge Kaplan is sufficiently widespread – and it requires only a look at the daily newspaper 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 periodic outbreaks of crisis.

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 Panopticon – not as an organizing metaphor for discipline in the information age, but in its original and more limited sense 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. In the particular case of the prison, the instrumentalities of crisis discipline are geographically contained, but the point is a more general one: Normal discipline and crisis discipline are not mutually exclusive states, and their boundaries will constantly be subject to (re)negotiation.⁷⁷

More generally, from the perspective of structuration theory, a model of discipline that envisions the simple substitution of “normal” modalities for crisis modalities would be too simple. Resolution of crisis may be expected to produce new relations of power and new recursive practices among groups of actors, both of which are unlikely to dissolve without a trace once crisis is resolved. In the particular case of crisis DRM, these new relationships and practices would also flow from the implementation of new technical standards, which would

⁷⁶ 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 ‘ordinary’ and the ‘normal.’” Gross, *supra*, at 1069-96. Ackerman concurs, but believes that extent to which crisis mentality becomes normalized will depend rather substantially on how “emergency” is understood. Ackerman, *supra*, at 1039-45. As the remainder of this essay will suggest, I believe both are right.

⁷⁷ Cf. Ackerman, *supra* note ___, at 1045 (contrasting “[b]ad legal structures” that “channel temporary needs for reassurance into permanent restrictions on liberty” with “good structures [that] will channel them into temporary states of emergency”). The question, as Ackerman recognizes, is whether this can be accomplished “without permanent damage to fundamental freedoms.” *Id.*

NORMAL DISCIPLINE IN THE AGE OF CRISIS

produce lock-in effects roughly proportionate to their degree of embeddedness within general purpose platforms and networking protocols. In the digital age, plague control may be expensive to implement but equally expensive to remove.⁷⁸

What DRM technologies and related information control strategies are designed to make possible is precisely a fusion of the exigency model with the generalizable model to produce a hybrid of the two: generalizable discipline designed to keep ever-looming crisis at bay. Fundamental to this regulatory model is the capacity to instantiate lock-down, and to “kill that which moves,” on the justification that the state of emergency is always with us. Equally fundamental, the model is a means of instilling in consumers an unquestioning acceptance of both the particular boundaries, and a particular overarching conception of boundedness, that content owners want. Rights management protocols designed to forestall crisis pursue a double-pronged strategy consisting of the simultaneous gathering of information and the invasion and rigid partitioning of (virtual) space. They simultaneously redraw the boundaries of private territory; rather than normalizing those who remain on the “right” side of the new boundaries, however, it is the universality of the boundaries themselves that becomes normal.

Within the new disciplinary paradigm of normalized exigency, the unevenness of our emerging boundary principles makes sense. Quite simply, it is the price we are asked to pay, willingly or no, to avert what is portrayed as a massive economic meltdown. The ability to extract proprietary information without paying the expected price and leaving the expected data trail is part of the disease that lurks at our virtual doorsteps. Measured by this standard, imposing comparable restrictions on content proprietors would serve no useful purpose.

The normal discipline described by Foucault weighs least heavily on the normal; that is both its point and its method. For the reasons just explained, though, the normal discipline exemplified by crisis DRM does not entirely fit this pattern. The restrictions are designed to bind everyone, and ensure that everyone is monitored. The shift to crisis DRM thus holds the potential to accomplish a breathtakingly inclusive extension of surveillance and control, of the type that Foucault’s medieval rulers might have wished, but did not dare, to put in place. To characterize this extension simply as a “shift in the cultural baseline,” as some of its proponents have suggested, is to trivialize its magnitude and fundamentally misapprehend its operation.

VI. CRISIS DISCIPLINE AS SPATIAL PRACTICE

Thus far, I have simply attempted to describe the emerging social phenomenon of crisis DRM and locate it within an historical continuum of disciplinary practices, without questioning the logic of the disease metaphor as applied to online copyright infringement. It is time to take stock. Surveillance and direct enforcement of restrictions on intellectual goods are not necessary

⁷⁸ See Joan Feigenbaum, et al., *Privacy Engineering for Digital Rights Management Systems in* PROCEEDINGS OF THE 2001 ACM WORKSHOP ON SECURITY AND PRIVACY IN DIGITAL RIGHTS MANAGEMENT 76 (2002).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

to anyone's survival in the literal, physical sense; at least so far, no one has died of online copyright infringement. Yet perceived threats to commerce in information may become the entering wedge for what literally life-threatening conditions could not achieve: a regime of precise and permanent oversight and control. How should we think about the discipline that this vision, if brought to fruition, would inculcate?

Answering this question requires careful consideration of both the claimed benefits of crisis DRM 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: namely, institutions that apply (and act upon) shared values to mediate and structure human interactions. 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 mode would serve a broader range of productive interests, and whether it would further or frustrate important noninstrumental values.

To the extent that crisis discipline enables detection 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. 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 the pressures of change.

The extent of both benefits, however, is open to considerable debate. Many people argue that a system of intellectual property protection produces the greatest benefits when rules granting protection are balanced by offsetting limits. One can acknowledge the potential benefits of "better" intellectual property enforcement while still reserving rather substantial questions about how much enforcement is best. Similarly, some resolutions of crisis are more productive than others. For purposes of this essay, I will bracket the first problem and focus on the second. Let us consider now some additional entailments of the normalization of this particular mode of crisis discipline.

First and most obviously, the deployment and normalization of crisis functionality will affect individual freedom in important ways; that is, after all, its stated purpose. Direct functionality restrictions intrude on the seclusion, or "private space," that social practice reserves to the individual, and substantially shift the baseline conditions of user autonomy to determine

NORMAL DISCIPLINE IN THE AGE OF CRISIS

the circumstances of use and enjoyment of intellectual goods.⁷⁹ They therefore constrain freedom in both its positive and negative senses; one may take only certain actions with authorized copies of intellectual goods. Punitive self-help measures leave individuals vulnerable to losing even the small remaining range of freedom permitted.

Surveillance of intellectual consumption brings to bear a second, more subtle set of behavioral and intellectual constraints. Information about intellectual activity has long been regarded as fundamentally private, both for reasons related to individual dignity and because of the powerful chilling effect that disclosure of intellectual preferences can produce. At least in some cases, persistent collection of this information will cause individuals to limit the scope of their own intellectual, cultural, and political exploration.⁸⁰ Use of collected preference information to funnel particular intellectual goods to particular recipients can intensify this dynamic.⁸¹ At the same time, the likelihood of being targeted by vigilante searches for unauthorized content may further constrain other, potentially lawful, uses of intellectual goods.

If one keeps in mind that the central concern of crisis DRM is discipline, as opposed to simple prohibition, none of this should come as a great surprise. Foucault reminds us that surveillance and rank-ordering can be effective disciplinary substitutes for more extreme measures of social control, and that this is so not only in prisons and police states, but also in schools, where these techniques are deployed to inculcate nothing more sinister than “normal” socialization. For anyone raised in a real, time- and place-bound society, some external structuring of intellectual development is inevitable, and even good. Nonetheless, the techniques of crisis DRM betoken a qualitative shift in the extent and nature of the feedback process that operates at the “normal” end of the spectrum.

More fundamentally and concretely, the instantiation of crisis functionality will affect the production of space as experienced by individual users of information goods. The progressive insertion of control and surveillance into private spaces changes both the experience of those spaces and the experience of the wider information environment that includes the Internet and its constituent networks.

Cyberlaw scholars are increasingly attentive to the uses and misuses of spatial metaphors for communications networks.⁸² The utopian dreams of Internet pioneers notwithstanding, it

⁷⁹ For a more extended development of this point, see Cohen, *supra* note __, at 580-83 (arguing that automated DRM restrictions affect both liberty and privacy interests).

⁸⁰ See Cohen, *supra* note __; Cohen, *supra* note __, at 584-86.

⁸¹ I am less concerned here with the “Daily Me” than with the “Daily You” and its relation to the “Daily Us.” Compare CASS R. SUNSTEIN, *REPUBLIC.COM* (2001), with EDWARD S. HERMAN & NOAM CHOMSKY, *MANUFACTURING CONSENT: THE POLITICAL ECONOMY OF THE MASS MEDIA* (1988).

⁸² See, e.g., Dan L. Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439 (2003); Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003); Timothy Wu, *When Law*

NORMAL DISCIPLINE IN THE AGE OF CRISIS

now seems established that the Internet is not a separate place in either the physical or the jurisdictional sense. Even so, there are two different and equally important respects in which attention to spatialization is essential to the project of constructing rules for the information age.

First, research in human cognition demonstrates that humans are innately spatially-oriented beings.⁸³ We apply spatial metaphors to a wide range of social phenomena that do not map neatly to physical x, y, and z coordinates because that is how our brains and bodies work. Even in the disembodied medium of the Internet, information is experienced, processed, and reproduced through and in relation to the body.⁸⁴ On the network we surf, lurk, post messages on boards, and access domains and mailboxes; within our private computing environments we consume cultural products, absorb and digest facts and opinions, and rip, mix, and burn sounds and images. While this does not mean we cannot distinguish between metaphor and reality, or that we cannot change culturally dominant spatial metaphors and learn to use different ones, it does mean that more formal efforts to develop a spatialized understanding of the networked information “environment” make a good deal of sense. It means, as well, that asserting agency, or more properly subjectivity, as to the rules of engagement between the network and the self is a matter of vital importance.⁸⁵

The second set of insights into the importance of understanding information networks in spatial terms derives from postmodernist geography and historiography, which emphasizes the importance of space, as well as time, in understanding the development of human societies.⁸⁶ Individuals, firms, and social movements alike are situated in spaces as well as in times, and

and the Internet First Met, 3 GREEN BAG 171 (2000); Yen, *supra* note __; David MacGowan, *The Trespass Trouble and the Metaphor Muddle*, working paper (2004), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=521982>; Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357 (2003); Brett M. Frischmann, *The Prospect of Reconciling Internet and Cyberspace*, 35 LOY. U. CHI. L.J. 205 (2003); Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433 (2003)..

⁸³ See Hunter, *supra* note __; GEORGE LAKOFF & MARK JOHNSON, *METAPHORS WE LIVE BY* (1980); STEVEN WINTER, *A CLEARING IN THE FOREST: LAW, LIFE, AND THE MIND* (2001).

⁸⁴ As this formulation suggests, I suspect that scholars who study information networks have a thing or two to learn from critical feminism as well. In particular, 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 is shaped by the “informatics of domination.” DONNA J. HARAWAY, *SIMIAN, CYBORGS, AND WOMEN* 149-81 (1991).

⁸⁵ *Cf. id.* at 150-51 (imagining a “cyborg politics” that is “oppositional, utopian, and completely without innocence”); LAKOFF & JOHNSON, *supra* note __, at 185-94 (advancing a vision of understanding grounded in “imaginative rationality”).

⁸⁶ See MANUEL CASTELLS, *THE RISE OF THE NETWORK SOCIETY* 410-28 (1996); DAVID HARVEY, *THE CONDITION OF POSTMODERNITY: AN ENQUIRY INTO THE ORIGINS OF CULTURAL CHANGE* (1990); HENRI LEFEBVRE, *THE PRODUCTION OF SPACE* (1974, Donald Nicholson-Smith trans. 1991); EDWARD W. SOJA, *POSTMODERN GEOGRAPHIES: THE REASSERTION OF SPACE IN CRITICAL SOCIAL THEORY* (1989).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

economic and political success consist of the successful use of capital and/or political power to overcome both temporal and geographic constraints. Understanding the ways in which physical, economic, and symbolic power and practice shape the ongoing production of space within a society is vital to understanding both its history and the likely constraints on its future. Communications networks overcome space, but also create space – (metaphoric) zones of power and disempowerment, of access and exclusion, of opportunity and disadvantage. The drive toward progressive perfection of control over the movement of information within society must be evaluated, among other things, based on the geography of information spaces that it is likely to produce.

At the individual level, the insertion of control and surveillance into formerly private spaces redraws the boundary between private and public, producing at the boundary a third sort of space that is neither conventionally public nor entirely private, neither familiar nor wholly unfamiliar. The spaces of intellectual consumption under crisis DRM seem 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).⁸⁷

In aggregate, the discipline of control and surveillance produces standardized, homogenized space. Michael Madison has argued that, just as early twentieth century urban planning moved to eliminate visual chaos and replace it with order, so the contractually mediated standardization of information access threatens to eliminate the diversity of textures and “feels” that flourishes under less restrictive architectures.⁸⁸ This insight reaches beyond “information” abstracted from time and place, and indeed, on its own terms, it must reach more broadly. The shifting of intellectual activities out of the vibrant, chaotic diversity of specific, private spaces and uses into the controlled and standardized spaces of crisis DRM is in some respects comparable in feel to the replacement of mixed-use urban landscape with a large shopping mall or housing project. 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 unlike anything that the built physical environment has ever experienced.

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 pervasive interpolation of enforcement and surveillance functions into private spaces, and private intellectual activities conducted from within those spaces, works a kind of violence that is no less real because it is nonphysical. Robert Cover reminded us of the violence latent in symbolic

⁸⁷ Cf. HARAWAY, *supra* note __, at 163 (“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”).

⁸⁸ Michael J. Madison, *Complexity and Copyright in Contradiction*, 18 CARDOZO ARTS & ENT. L.J. 125 (2000).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

power.⁸⁹ Cover's thesis had to do with state capacity for violence and its sanitization by the ostensibly bloodless and civilized syntax of the law, but it is worth considering its implications here. In information spaces, there is only symbolic power; it is symbols deployed in the syntax of computer-executable code that cause information goods and networks, and the individuals who use them, to behave in particular ways. Code, we are told, regulates behavior – if not for everyone, then at least for most. When code works disruptions and invasions of sufficient enormity, arguably the bloodless and civilized label of “private ordering” no longer does them justice.

Although information goods and networks are designed, deployed, and operated (for the most part) by non-state actors, the state is centrally implicated in the violence worked by the deployment of crisis discipline. A core precept of liberal political theory is the state's obligation to prevent domination of the weak by the strong. If it declines to intervene in the pervasive restructuring of information spaces sought by crisis DRM, it shares responsibility for the result (and, not so incidentally, calls liberal political theory into serious question). And, as already discussed, in the case of intellectual property enforcement, the state has done far more than simply sit by. State sovereigns are not indifferent to the possibility of inserting control and surveillance functions into communications networks.⁹⁰ 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. The adaptation and territorialization of control and surveillance functions can empower sovereigns to combat purely local plagues – pornography, or hate speech, or terrorism, or dissent. Through crisis DRM, state sovereigns may realize their own dreams of control after all, and far more easily than they could have done directly.

From the standpoint of information 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. If the necessary consequence of embracing crisis DRM is perfect discipline and the necessary consequence of refusing it is the collapse of information markets and the premature demise of the Information Society, we face an unenviable choice.

VII. CHOICES, SMALL AND LARGE

Surely, though, it is going a bit far to say that the discipline of crisis DRM strips individuals of whatever agency and whatever private space they possess? There is, after all, a certain irony in structuralist defenses of individual freedom.⁹¹ If we are to take individual

⁸⁹ Robert Cover, *Violence and the Word*, 95 YALE L.J. 1601 (1986); see also PIERRE BOURDIEU, PRACTICAL REASON 45-60 (1998) (discussing the origins and operation of symbolic power).

⁹⁰ See Birnhack & Elkin-Koren, *supra* note __.

⁹¹ For a particularly insightful version of this critique, see DAVID LUBAN, LEGAL MODERNISM (1997).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

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, that 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.⁹² So too even under crisis DRM. Many of the measures described above are aspirational; there are no guarantees that they will find acceptance among information consumers and no guarantees that they will work as claimed. Here the poststructuralist critique achieves an unlikely fusion with a distinctly cyberlibertarian vision of the agency of information users: If crisis DRM is this bad, people will refuse to buy it, and if it is foisted upon them, they will sabotage it.

In the literal sense, this critique is quite right. Most likely, even universal implementation of crisis DRM measures to the eighth and final level 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. Perfect panopticism, in other words, is unattainable. The digital world will remain a place where conflicting spatial practices and visions struggle for primacy.

Preventing all unauthorized uses of information, however, is not the point of crisis DRM, 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.⁹³ Normal discipline requires deviance constantly produced and carefully defined. Normal discipline in the age of crisis adopts as an additional leitmotif the specter of barely averted, always imminent collapse. The darknet serves both needs.

The interplay between crisis DRM and the darknet nonetheless will shape in distinct, and distinctly dystopian, ways 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.⁹⁴ In conditions of postmodernity, which are characterized in part

⁹² See Rosemary J. Coombe, *THE CULTURAL LIFE OF INTELLECTUAL PROPERTIES: AUTHORSHIP, APPROPRIATION, AND THE LAW* (1998); David Lange & Jennifer Lange Anderson, *Copyright, Fair Use and Transformative Critical Appropriation*, working paper (2001), <<http://www.law.duke.edu/pd/papers/langeand.pdf>>; Negativland, *Two Relations to a Cultural Public Domain*, 33 L. & CONTEMP. PROBS. 239 (2003).

⁹³ See FOUCAULT, *DISCIPLINE AND PUNISH*, *supra* note __, at 82-103.

⁹⁴ COOMBE, *supra* note __.

NORMAL DISCIPLINE IN THE AGE OF CRISIS

by the accumulation of informational capital and its exchange via global communications networks, these rules trend inexorably toward increasing constriction even as the popular claim of right to engage in acts of creative (or destructive) appropriation becomes more acute. This is doubly true of the mechanisms that extend automatic enforcement of those rules into the spaces of intellectual consumption, and therefore affect not only the legality but also the literal feasibility of resistance. In both its exigent and normal modalities, crisis DRM operates upon difference and resistance to produce homogenous, abstract, carefully controlled space, within which even difference and resistance follow more narrowly prescribed paths.⁹⁵

From a less overtly oppositional perspective, 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.⁹⁶ Crisis DRM elides the difference between public/rule-governed behavior and private behavior that is far more loosely circumscribed by applicable rules and social norms. Some offenses, most notably crimes against persons, are so severe that they may be thought to justify such elision.⁹⁷ In other cases, though, 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.⁹⁸

Neither the postmodern counterhegemon nor the law-creating citizen fares especially well under conditions of crisis discipline. Crisis discipline mediated through and by the information environment narrowly circumscribes the possibility for opposition, deliberative dialogue, and everything in between. Learning to live, at least in part, within these new spaces of intellectual consumption will require a different set of habits and social practices than the ones we currently have. Beyond science fiction, it is not clear whether we have the tools to understand fully what these might be.⁹⁹ It is reasonably clear, however, that these costs of crisis DRM should not lightly be dismissed as insignificant, or as wholly subject to nullification through interstitial strategies of resistance.

⁹⁵ Cf. LEFEBVRE, *supra* note __, at 319-20 (“[I]n a brightly illuminated night the day’s prohibitions give way to profitable transgressions.”).

⁹⁶ An earlier version of this argument appears in Cohen, *supra* note __, at 587-88.

⁹⁷ It is worth noting, however, that we are far from certain about this. In particular, Anthony Burgess’s *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.

⁹⁸ See Robert Cover, *The Supreme Court, 1982 Term – Foreword: Nomos and Narrative*, 97 HARV. L. REV. 4 (1983).

⁹⁹ For one such effort, see Richard Stallman, *The Right to Read*, 40 COMM. ACM 85-87 (1997).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

Focusing exclusively on interstitial strategies of resistance is short-sighted for a second and far more important reason: It ignores the antecedent question whether the shift to a full-blown implementation of crisis DRM is even necessary. Adaptation strategies matter most if there is no 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 frequently entail compromise. It would be odd if the advent of digital 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 crisis discipline and information anarchy. Such is the level of organized hysteria surrounding online “theft” of copyrighted materials, and the concomitant mystification surrounding the development and deployment of technical standards for DRM, however, that the public debate has largely ignored the possibility of a middle ground.

In a more abstract sense, the question that needs to be answered is whether the technologies of DRM 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.¹⁰⁰ This question parallels those posed by a number of scholars about prevailing modalities for understanding intellectual property ownership and information privacy, and about the interaction between the design of network technologies and freedom of speech.¹⁰¹

We have not done nearly enough, at either the conceptual or the practical level, to know the answer to this sort of question. At the conceptual level, what is missing from current thinking about ownership, control, and processing of information is a rigorous inquiry into the

¹⁰⁰ 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 __, at 325-35 (calling for an “epistemological Luddism” that would consider “at least the following: (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 a preliminary exploration of this question in the context of DRM technologies, see Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41 (2001).

¹⁰¹ See, e.g., LESSIG, *supra* note __; Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395 (1999); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn’t Get)*, 2001 STAN. TECH. L. REV. 1; Paul M. Schwartz, *Beyond Lessig’s Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743 (2000).

NORMAL DISCIPLINE IN THE AGE OF CRISIS

feasibility of, and possible normative justifications for, “settling” for imperfection.¹⁰² Or, to put it differently, what we lack is a framework for considering whether striving for imperfection might not constitute “settling” at all. The conceptual shifts entailed in developing such a framework, and the practical challenges entailed in operationalizing it, demand our serious attention.

¹⁰² Recent proposals to protect digital copyright entitlements with liability rules are a welcome step in this direction. See WILLIAM W. FISHER, *PROMISES TO KEEP* (forthcoming 2004); Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J.L. & TECH. 1 (2003).